

States under false pretenses for the purpose of collecting intelligence to inform the ORGANIZATION's operations.

16. Defendant SERGEY PAVLOVICH POLOZOV (Полозов Сергей Павлович) worked for the ORGANIZATION from at least in or around April 2014 to at least in or around October 2016. POLOZOV served as the manager of the IT department and oversaw the procurement of U.S. servers and other computer infrastructure that masked the ORGANIZATION's Russian location when conducting operations within the United States.

17. Defendant ANNA VLADISLAVOVNA BOGACHEVA (Богачева Анна Владиславовна) worked for the ORGANIZATION from at least in or around April 2014 to at least in or around July 2014. BOGACHEVA served on the translator project and oversaw the project's data analysis group. BOGACHEVA also traveled to the United States under false pretenses for the purpose of collecting intelligence to inform the ORGANIZATION's operations.

18. Defendant MARIA ANATOLYEVNA BOVDA (Бовда Мария Анатольевна) A/K/A MARIA ANATOLYEVNA BELYAEVA ("M. BOVDA") worked for the ORGANIZATION from at least in or around November 2013 to at least in or around October 2014. M. BOVDA served as the head of the translator project, among other positions.

19. Defendant ROBERT SERGEYEVICH BOVDA (Бовда Роберт Сергеевич) ("R. BOVDA") worked for the ORGANIZATION from at least in or around November 2013 to at least in or around October 2014. R. BOVDA served as the deputy head of the translator project, among other positions. R. BOVDA attempted to travel to the United States under false pretenses for the purpose of collecting intelligence to inform the ORGANIZATION's operations but could not obtain the necessary visa.

20. Defendant DZHEYKHUN NASIMI OGLY ASLANOV (Асланов Джейхун Насими Оглы) A/K/A JAYHOON ASLANOV A/K/A JAY ASLANOV joined the ORGANIZATION by at least in or around September 2014. ASLANOV served as head of the translator project and oversaw many of the operations targeting the 2016 U.S. presidential election. ASLANOV was also listed as the general director of Azimut LLC, an entity used to move funds from CONCORD to the ORGANIZATION.

21. Defendant VADIM VLADIMIROVICH PODKOPEV (Подкопаев Вадим Владимирович) joined the ORGANIZATION by at least in or around June 2014. PODKOPEV served as an analyst on the translator project and was responsible for conducting U.S.-focused research and drafting social media content for the ORGANIZATION.

22. Defendant GLEB IGOREVICH VASILCHENKO (Васильченко Глеб Игоревич) worked for the ORGANIZATION from at least in or around August 2014 to at least in or around September 2016. VASILCHENKO was responsible for posting, monitoring, and updating the social media content of many ORGANIZATION-controlled accounts while posing as U.S. persons or U.S. grassroots organizations. VASILCHENKO later served as the head of two sub-groups focused on operations to interfere in the U.S. political system, including the 2016 U.S. presidential election.

23. Defendant IRINA VIKTOROVNA KAVERZINA (Каверзина Ирина Викторовна) joined the ORGANIZATION by at least in or around October 2014. KAVERZINA served on the translator project and operated multiple U.S. personas that she used to post, monitor, and update social media content for the ORGANIZATION.

24. Defendant VLADIMIR VENKOV (Венков Владимир) joined the ORGANIZATION by at least in or around March 2015. VENKOV served on the translator project and operated multiple

U.S. personas, which he used to post, monitor, and update social media content for the ORGANIZATION.

### **Federal Regulatory Agencies**

25. The Federal Election Commission is a federal agency that administers the Federal Election Campaign Act (“FECA”). Among other things, FECA prohibits foreign nationals from making any contributions, expenditures, independent expenditures, or disbursements for electioneering communications. FECA also requires that individuals or entities who make certain independent expenditures in federal elections report those expenditures to the Federal Election Commission. The reporting requirements permit the Federal Election Commission to fulfill its statutory duties of providing the American public with accurate data about the financial activities of individuals and entities supporting federal candidates, and enforcing FECA’s limits and prohibitions, including the ban on foreign expenditures.

26. The U.S. Department of Justice administers the Foreign Agent Registration Act (“FARA”). FARA establishes a registration, reporting, and disclosure regime for agents of foreign principals (which includes foreign non-government individuals and entities) so that the U.S. government and the people of the United States are informed of the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and law. FARA requires, among other things, that persons subject to its requirements submit periodic registration statements containing truthful information about their activities and the income earned from them. Disclosure of the required information allows the federal government and the American people to evaluate the statements and activities of such persons in light of their function as foreign agents.

27. The U.S. Department of State is the federal agency responsible for the issuance of non-immigrant visas to foreign individuals who need a visa to enter the United States. Foreign

individuals who are required to obtain a visa must, among other things, provide truthful information in response to questions on the visa application form, including information about their employment and the purpose of their visit to the United States.

**Object of the Conspiracy**

28. The conspiracy had as its object impairing, obstructing, and defeating the lawful governmental functions of the United States by dishonest means in order to enable the Defendants to interfere with U.S. political and electoral processes, including the 2016 U.S. presidential election.

**Manner and Means of the Conspiracy**

**Intelligence-Gathering to Inform U.S. Operations**

29. Starting at least in or around 2014, Defendants and their co-conspirators began to track and study groups on U.S. social media sites dedicated to U.S. politics and social issues. In order to gauge the performance of various groups on social media sites, the ORGANIZATION tracked certain metrics like the group's size, the frequency of content placed by the group, and the level of audience engagement with that content, such as the average number of comments or responses to a post.

30. Defendants and their co-conspirators also traveled, and attempted to travel, to the United States under false pretenses in order to collect intelligence for their interference operations.

- a. KRYLOVA and BOGACHEVA, together with other Defendants and co-conspirators, planned travel itineraries, purchased equipment (such as cameras, SIM cards, and drop phones), and discussed security measures (including "evacuation scenarios") for Defendants who traveled to the United States.
- b. To enter the United States, KRYLOVA, BOGACHEVA, R. BOVDA, and another co-conspirator applied to the U.S. Department of State for visas to travel. During

their application process, KRYLOVA, BOGACHEVA, R. BOVDA, and their co-conspirator falsely claimed they were traveling for personal reasons and did not fully disclose their place of employment to hide the fact that they worked for the ORGANIZATION.

- c. Only KRYLOVA and BOGACHEVA received visas, and from approximately June 4, 2014 through June 26, 2014, KRYLOVA and BOGACHEVA traveled in and around the United States, including stops in Nevada, California, New Mexico, Colorado, Illinois, Michigan, Louisiana, Texas, and New York to gather intelligence. After the trip, KRYLOVA and BURCHIK exchanged an intelligence report regarding the trip.
- d. Another co-conspirator who worked for the ORGANIZATION traveled to Atlanta, Georgia from approximately November 26, 2014 through November 30, 2014. Following the trip, the co-conspirator provided POLOZOV a summary of his trip's itinerary and expenses.

31. In order to collect additional intelligence, Defendants and their co-conspirators posed as U.S. persons and contacted U.S. political and social activists. For example, starting in or around June 2016, Defendants and their co-conspirators, posing online as U.S. persons, communicated with a real U.S. person affiliated with a Texas-based grassroots organization. During the exchange, Defendants and their co-conspirators learned from the real U.S. person that they should focus their activities on "purple states like Colorado, Virginia & Florida." After that exchange, Defendants and their co-conspirators commonly referred to targeting "purple states" in directing their efforts.

Use of U.S. Social Media Platforms

32. Defendants and their co-conspirators, through fraud and deceit, created hundreds of social media accounts and used them to develop certain fictitious U.S. personas into “leader[s] of public opinion” in the United States.

33. ORGANIZATION employees, referred to as “specialists,” were tasked to create social media accounts that appeared to be operated by U.S. persons. The specialists were divided into day-shift and night-shift hours and instructed to make posts in accordance with the appropriate U.S. time zone. The ORGANIZATION also circulated lists of U.S. holidays so that specialists could develop and post appropriate account activity. Specialists were instructed to write about topics germane to the United States such as U.S. foreign policy and U.S. economic issues. Specialists were directed to create “political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements.”

34. Defendants and their co-conspirators also created thematic group pages on social media sites, particularly on the social media platforms Facebook and Instagram. ORGANIZATION-controlled pages addressed a range of issues, including: immigration (with group names including “Secured Borders”); the Black Lives Matter movement (with group names including “Blacktivist”); religion (with group names including “United Muslims of America” and “Army of Jesus”); and certain geographic regions within the United States (with group names including “South United” and “Heart of Texas”). By 2016, the size of many ORGANIZATION-controlled groups had grown to hundreds of thousands of online followers.

35. Starting at least in or around 2015, Defendants and their co-conspirators began to purchase advertisements on online social media sites to promote ORGANIZATION-controlled social media groups, spending thousands of U.S. dollars every month. These expenditures were included in the budgets the ORGANIZATION submitted to CONCORD.

36. Defendants and their co-conspirators also created and controlled numerous Twitter accounts designed to appear as if U.S. persons or groups controlled them. For example, the ORGANIZATION created and controlled the Twitter account “Tennessee GOP,” which used the handle @TEN\_GOP. The @TEN\_GOP account falsely claimed to be controlled by a U.S. state political party. Over time, the @TEN\_GOP account attracted more than 100,000 online followers.

37. To measure the impact of their online social media operations, Defendants and their co-conspirators tracked the performance of content they posted over social media. They tracked the size of the online U.S. audiences reached through posts, different types of engagement with the posts (such as likes, comments, and reposts), changes in audience size, and other metrics. Defendants and their co-conspirators received and maintained metrics reports on certain group pages and individualized posts.

38. Defendants and their co-conspirators also regularly evaluated the content posted by specialists (sometimes referred to as “content analysis”) to ensure they appeared authentic—as if operated by U.S. persons. Specialists received feedback and directions to improve the quality of their posts. Defendants and their co-conspirators issued or received guidance on: ratios of text, graphics, and video to use in posts; the number of accounts to operate; and the role of each account (for example, differentiating a main account from which to post information and auxiliary accounts to promote a main account through links and reposts).

#### Use of U.S. Computer Infrastructure

39. To hide their Russian identities and ORGANIZATION affiliation, Defendants and their co-conspirators—particularly POLOZOV and the ORGANIZATION’s IT department—purchased space on computer servers located inside the United States in order to set up virtual private networks (“VPNs”). Defendants and their co-conspirators connected from Russia to the U.S.-

based infrastructure by way of these VPNs and conducted activity inside the United States—including accessing online social media accounts, opening new accounts, and communicating with real U.S. persons—while masking the Russian origin and control of the activity.

40. Defendants and their co-conspirators also registered and controlled hundreds of web-based email accounts hosted by U.S. email providers under false names so as to appear to be U.S. persons and groups. From these accounts, Defendants and their co-conspirators registered or linked to online social media accounts in order to monitor them; posed as U.S. persons when requesting assistance from real U.S. persons; contacted media outlets in order to promote activities inside the United States; and conducted other operations, such as those set forth below.

#### Use of Stolen U.S. Identities

41. In or around 2016, Defendants and their co-conspirators also used, possessed, and transferred, without lawful authority, the social security numbers and dates of birth of real U.S. persons without those persons' knowledge or consent. Using these means of identification, Defendants and their co-conspirators opened accounts at PayPal, a digital payment service provider; created false means of identification, including fake driver's licenses; and posted on ORGANIZATION-controlled social media accounts using the identities of these U.S. victims. Defendants and their co-conspirators also obtained, and attempted to obtain, false identification documents to use as proof of identity in connection with maintaining accounts and purchasing advertisements on social media sites.

#### Actions Targeting the 2016 U.S. Presidential Election

42. By approximately May 2014, Defendants and their co-conspirators discussed efforts to interfere in the 2016 U.S. presidential election. Defendants and their co-conspirators began to monitor U.S. social media accounts and other sources of information about the 2016 U.S. presidential election.

43. By 2016, Defendants and their co-conspirators used their fictitious online personas to interfere with the 2016 U.S. presidential election. They engaged in operations primarily intended to communicate derogatory information about Hillary Clinton, to denigrate other candidates such as Ted Cruz and Marco Rubio, and to support Bernie Sanders and then-candidate Donald Trump.

- a. On or about February 10, 2016, Defendants and their co-conspirators internally circulated an outline of themes for future content to be posted to ORGANIZATION-controlled social media accounts. Specialists were instructed to post content that focused on “politics in the USA” and to “use any opportunity to criticize Hillary and the rest (except Sanders and Trump—we support them).”
- b. On or about September 14, 2016, in an internal review of an ORGANIZATION-created and controlled Facebook group called “Secured Borders,” the account specialist was criticized for having a “low number of posts dedicated to criticizing Hillary Clinton” and was told “it is imperative to intensify criticizing Hillary Clinton” in future posts.

44. Certain ORGANIZATION-produced materials about the 2016 U.S. presidential election used election-related hashtags, including: “#Trump2016,” “#TrumpTrain,” “#MAGA,” “#IWontProtectHillary,” and “#Hillary4Prison.” Defendants and their co-conspirators also established additional online social media accounts dedicated to the 2016 U.S. presidential election, including the Twitter account “March for Trump” and Facebook accounts “Clinton FRAUDation” and “Trumpsters United.”

45. Defendants and their co-conspirators also used false U.S. personas to communicate with unwitting members, volunteers, and supporters of the Trump Campaign involved in local community outreach, as well as grassroots groups that supported then-candidate Trump. These

individuals and entities at times distributed the ORGANIZATION's materials through their own accounts via retweets, reposts, and similar means. Defendants and their co-conspirators then monitored the propagation of content through such participants.

46. In or around the latter half of 2016, Defendants and their co-conspirators, through their ORGANIZATION-controlled personas, began to encourage U.S. minority groups not to vote in the 2016 U.S. presidential election or to vote for a third-party U.S. presidential candidate.

- a. On or about October 16, 2016, Defendants and their co-conspirators used the ORGANIZATION-controlled Instagram account "Woke Blacks" to post the following message: "[A] particular hype and hatred for Trump is misleading the people and forcing Blacks to vote Killary. We cannot resort to the lesser of two devils. Then we'd surely be better off without voting AT ALL."
- b. On or about November 3, 2016, Defendants and their co-conspirators purchased an advertisement to promote a post on the ORGANIZATION-controlled Instagram account "Blacktivist" that read in part: "Choose peace and vote for Jill Stein. Trust me, it's not a wasted vote."
- c. By in or around early November 2016, Defendants and their co-conspirators used the ORGANIZATION-controlled "United Muslims of America" social media accounts to post anti-vote messages such as: "American Muslims [are] boycotting elections today, most of the American Muslim voters refuse to vote for Hillary Clinton because she wants to continue the war on Muslims in the middle east and voted yes for invading Iraq."

47. Starting in or around the summer of 2016, Defendants and their co-conspirators also began to promote allegations of voter fraud by the Democratic Party through their fictitious U.S. personas

and groups on social media. Defendants and their co-conspirators purchased advertisements on Facebook to further promote the allegations.

- a. On or about August 4, 2016, Defendants and their co-conspirators began purchasing advertisements that promoted a post on the ORGANIZATION-controlled Facebook account “Stop A.I.” The post alleged that “Hillary Clinton has already committed voter fraud during the Democrat Iowa Caucus.”
- b. On or about August 11, 2016, Defendants and their co-conspirators posted that allegations of voter fraud were being investigated in North Carolina on the ORGANIZATION-controlled Twitter account @TEN\_GOP.
- c. On or about November 2, 2016, Defendants and their co-conspirators used the same account to post allegations of “#VoterFraud by counting tens of thousands of ineligible mail in Hillary votes being reported in Broward County, Florida.”

#### Political Advertisements

48. From at least April 2016 through November 2016, Defendants and their co-conspirators, while concealing their Russian identities and ORGANIZATION affiliation through false personas, began to produce, purchase, and post advertisements on U.S. social media and other online sites expressly advocating for the election of then-candidate Trump or expressly opposing Clinton. Defendants and their co-conspirators did not report their expenditures to the Federal Election Commission, or register as foreign agents with the U.S. Department of Justice.

49. To pay for the political advertisements, Defendants and their co-conspirators established various Russian bank accounts and credit cards, often registered in the names of fictitious U.S. personas created and used by the ORGANIZATION on social media. Defendants and their co-conspirators also paid for other political advertisements using PayPal accounts.

50. The political advertisements included the following:

Approximate Date	Excerpt of Advertisement
April 6, 2016	"You know, a great number of black people support us saying that #HillaryClintonIsNotMyPresident"
April 7, 2016	"I say no to Hillary Clinton / I say no to manipulation"
April 19, 2016	"JOIN our #HillaryClintonForPrison2016"
May 10, 2016	"Donald wants to defeat terrorism . . . Hillary wants to sponsor it"
May 19, 2016	"Vote Republican, vote Trump, and support the Second Amendment!"
May 24, 2016	"Hillary Clinton Doesn't Deserve the Black Vote"
June 7, 2016	"Trump is our only hope for a better future!"
June 30, 2016	"#NeverHillary #HillaryForPrison #Hillary4Prison #HillaryForPrison2016 #Trump2016 #Trump #Trump4President"
July 20, 2016	"Ohio Wants Hillary 4 Prison"
August 4, 2016	"Hillary Clinton has already committed voter fraud during the Democrat Iowa Caucus."
August 10, 2016	"We cannot trust Hillary to take care of our veterans!"
October 14, 2016	"Among all the candidates Donald Trump is the one and only who can defend the police from terrorists."
October 19, 2016	"Hillary is a Satan, and her crimes and lies had proved just how evil she is."

#### Staging U.S. Political Rallies in the United States

51. Starting in approximately June 2016, Defendants and their co-conspirators organized and coordinated political rallies in the United States. To conceal the fact that they were based in Russia, Defendants and their co-conspirators promoted these rallies while pretending to be U.S. grassroots activists who were located in the United States but unable to meet or participate in person.

Defendants and their co-conspirators did not register as foreign agents with the U.S. Department of Justice.

52. In order to build attendance for the rallies, Defendants and their co-conspirators promoted the events through public posts on their false U.S. persona social media accounts. In addition, Defendants and their co-conspirators contacted administrators of large social media groups focused on U.S. politics and requested that they advertise the rallies.

53. In or around late June 2016, Defendants and their co-conspirators used the Facebook group “United Muslims of America” to promote a rally called “Support Hillary. Save American Muslims” held on July 9, 2016 in the District of Columbia. Defendants and their co-conspirators recruited a real U.S. person to hold a sign depicting Clinton and a quote attributed to her stating “I think Sharia Law will be a powerful new direction of freedom.” Within three weeks, on or about July 26, 2016, Defendants and their co-conspirators posted on the same Facebook page that Muslim voters were “between Hillary Clinton and a hard place.”

54. In or around June and July 2016, Defendants and their co-conspirators used the Facebook group “Being Patriotic,” the Twitter account @March\_for\_Trump, and other ORGANIZATION accounts to organize two political rallies in New York. The first rally was called “March for Trump” and held on June 25, 2016. The second rally was called “Down with Hillary” and held on July 23, 2016.

- a. In or around June through July 2016, Defendants and their co-conspirators purchased advertisements on Facebook to promote the “March for Trump” and “Down with Hillary” rallies.
- b. Defendants and their co-conspirators used false U.S. personas to send individualized messages to real U.S. persons to request that they participate in and

help organize the rally. To assist their efforts, Defendants and their co-conspirators, through false U.S. personas, offered money to certain U.S. persons to cover rally expenses.

- c. On or about June 5, 2016, Defendants and their co-conspirators, while posing as a U.S. grassroots activist, used the account @March\_for\_Trump to contact a volunteer for the Trump Campaign in New York. The volunteer agreed to provide signs for the “March for Trump” rally.

55. In or around late July 2016, Defendants and their co-conspirators used the Facebook group “Being Patriotic,” the Twitter account @March\_for\_Trump, and other false U.S. personas to organize a series of coordinated rallies in Florida. The rallies were collectively referred to as “Florida Goes Trump” and held on August 20, 2016.

- a. In or around August 2016, Defendants and their co-conspirators used false U.S. personas to communicate with Trump Campaign staff involved in local community outreach about the “Florida Goes Trump” rallies.
- b. Defendants and their co-conspirators purchased advertisements on Facebook and Instagram to promote the “Florida Goes Trump” rallies.
- c. Defendants and their co-conspirators also used false U.S. personas to contact multiple grassroots groups supporting then-candidate Trump in an unofficial capacity. Many of these groups agreed to participate in the “Florida Goes Trump” rallies and serve as local coordinators.
- d. Defendants and their co-conspirators also used false U.S. personas to ask real U.S. persons to participate in the “Florida Goes Trump” rallies. Defendants and their co-conspirators asked certain of these individuals to perform tasks at the rallies.

For example, Defendants and their co-conspirators asked one U.S. person to build a cage on a flatbed truck and another U.S. person to wear a costume portraying Clinton in a prison uniform. Defendants and their co-conspirators paid these individuals to complete the requests.

56. After the rallies in Florida, Defendants and their co-conspirators used false U.S. personas to organize and coordinate U.S. political rallies supporting then-candidate Trump in New York and Pennsylvania. Defendants and their co-conspirators used the same techniques to build and promote these rallies as they had in Florida, including: buying Facebook advertisements; paying U.S. persons to participate in, or perform certain tasks at, the rallies; and communicating with real U.S. persons and grassroots organizations supporting then-candidate Trump.

57. After the election of Donald Trump in or around November 2016, Defendants and their co-conspirators used false U.S. personas to organize and coordinate U.S. political rallies in support of then president-elect Trump, while simultaneously using other false U.S. personas to organize and coordinate U.S. political rallies protesting the results of the 2016 U.S. presidential election. For example, in or around November 2016, Defendants and their co-conspirators organized a rally in New York through one ORGANIZATION-controlled group designed to “show your support for President-Elect Donald Trump” held on or about November 12, 2016. At the same time, Defendants and their co-conspirators, through another ORGANIZATION-controlled group, organized a rally in New York called “Trump is NOT my President” held on or about November 12, 2016. Similarly, Defendants and their co-conspirators organized a rally entitled “Charlotte Against Trump” in Charlotte, North Carolina, held on or about November 19, 2016.

Destruction of Evidence

58. In order to avoid detection and impede investigation by U.S. authorities of Defendants' operations, Defendants and their co-conspirators deleted and destroyed data, including emails, social media accounts, and other evidence of their activities.

- a. Beginning in or around June 2014, and continuing into June 2015, public reporting began to identify operations conducted by the ORGANIZATION in the United States. In response, Defendants and their co-conspirators deleted email accounts used to conduct their operations.
- b. Beginning in or around September 2017, U.S. social media companies, starting with Facebook, publicly reported that they had identified Russian expenditures on their platforms to fund political and social advertisements. Facebook's initial disclosure of the Russian purchases occurred on or about September 6, 2017, and included a statement that Facebook had "shared [its] findings with US authorities investigating these issues."
- c. Media reporting on or about the same day as Facebook's disclosure referred to Facebook working with investigators for the Special Counsel's Office of the U.S. Department of Justice, which had been charged with investigating the Russian government's efforts to interfere in the 2016 presidential election.
- d. Defendants and their co-conspirators thereafter destroyed evidence for the purpose of impeding the investigation. On or about September 13, 2017, KAVERZINA wrote in an email to a family member: "We had a slight crisis here at work: the FBI busted our activity (not a joke). So, I got preoccupied with covering tracks together with the colleagues." KAVERZINA further wrote, "I created all these pictures and posts, and the Americans believed that it was written by their people."

**Overt Acts**

59. In furtherance of the Conspiracy and to effect its illegal object, Defendants and their co-conspirators committed the following overt acts in connection with the staging of U.S. political rallies, as well as those as set forth in paragraphs 1 through 7, 9 through 27, and 29 through 58, which are re-alleged and incorporated by reference as though fully set forth herein.

60. On or about June 1, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for their “March for Trump” rally.

61. On or about June 4, 2016, Defendants and their co-conspirators used allforusa@yahoo.com, the email address of a false U.S. persona, to send out press releases for the “March for Trump” rally to New York media outlets.

62. On or about June 23, 2016, Defendants and their co-conspirators used the Facebook account registered under a false U.S. persona “Matt Skiber” to contact a real U.S. person to serve as a recruiter for the “March for Trump” rally, offering to “give you money to print posters and get a megaphone.”

63. On or about June 24, 2016, Defendants and their co-conspirators purchased advertisements on Facebook to promote the “Support Hillary. Save American Muslims” rally.

64. On or about July 5, 2016, Defendants and their co-conspirators ordered posters for the “Support Hillary. Save American Muslims” rally, including the poster with the quote attributed to Clinton that read “I think Sharia Law will be a powerful new direction of freedom.”

65. On or about July 8, 2016, Defendants and their co-conspirators communicated with a real U.S. person about the posters they had ordered for the “Support Hillary. Save American Muslims” rally.

66. On or about July 12, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for the “Down With Hillary” rally in New York.

67. On or about July 23, 2016, Defendants and their co-conspirators used the email address of a false U.S. persona, joshmilton024@gmail.com, to send out press releases to over thirty media outlets promoting the “Down With Hillary” rally at Trump Tower in New York City.

68. On or about July 28, 2016, Defendants and their co-conspirators posted a series of tweets through the false U.S. persona account @March\_for\_Trump stating that “[w]e’re currently planning a series of rallies across the state of Florida” and seeking volunteers to assist.

69. On or about August 2, 2016, Defendants and their co-conspirators used the false U.S. persona “Matt Skiber” Facebook account to send a private message to a real Facebook account, “Florida for Trump,” set up to assist then-candidate Trump in the state of Florida. In the first message, Defendants and their co-conspirators wrote:

Hi there! I’m a member of Being Patriotic online community. Listen, we’ve got an idea. Florida is still a purple state and we need to paint it red. If we lose Florida, we lose America. We can’t let it happen, right? What about organizing a YUGE pro-Trump flash mob in every Florida town? We are currently reaching out to local activists and we’ve got the folks who are okay to be in charge of organizing their events almost everywhere in FL. However, we still need your support. What do you think about that? Are you in?

70. On or about August 2, 2016, and August 3, 2016, Defendants and their co-conspirators, through the use of a stolen identity of a real U.S. person, T.W., sent emails to certain grassroots groups located in Florida that stated in part:

My name is [T.W.] and I represent a conservative patriot community named as “Being Patriotic.” . . . So we’re gonna organize a flash mob across Florida to support Mr. Trump. We clearly understand that the elections winner will be predestined by purple states. And we must win Florida. . . . We got a lot of volunteers in ~25 locations and it’s just the beginning. We’re currently choosing venues for each

location and recruiting more activists. This is why we ask you to spread this info and participate in the flash mob.

71. On or about August 4, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for the “Florida Goes Trump” rally. The advertisements reached over 59,000 Facebook users in Florida, and over 8,300 Facebook users responded to the advertisements by clicking on it, which routed users to the ORGANIZATION’s “Being Patriotic” page.

72. Beginning on or about August 5, 2016, Defendants and their co-conspirators used the false U.S. persona @March\_for\_Trump Twitter account to recruit and later pay a real U.S. person to wear a costume portraying Clinton in a prison uniform at a rally in West Palm Beach.

73. Beginning on or about August 11, 2016, Defendants and their co-conspirators used the false U.S. persona “Matt Skiber” Facebook account to recruit a real U.S. person to acquire signs and a costume depicting Clinton in a prison uniform.

74. On or about August 15, 2016, Defendants and their co-conspirators received an email at one of their false U.S. persona accounts from a real U.S. person, a Florida-based political activist identified as the “Chair for the Trump Campaign” in a particular Florida county. The activist identified two additional sites in Florida for possible rallies. Defendants and their co-conspirators subsequently used their false U.S. persona accounts to communicate with the activist about logistics and an additional rally in Florida.

75. On or about August 16, 2016, Defendants and their co-conspirators used a false U.S. persona Instagram account connected to the ORGANIZATION-created group “Tea Party News” to purchase advertisements for the “Florida Goes Trump” rally.

76. On or about August 18, 2016, the real “Florida for Trump” Facebook account responded to the false U.S. persona “Matt Skiber” account with instructions to contact a member of the Trump Campaign (“Campaign Official 1”) involved in the campaign’s Florida operations and provided

Campaign Official 1's email address at the campaign domain donaldtrump.com. On approximately the same day, Defendants and their co-conspirators used the email address of a false U.S. persona, joshmilton024@gmail.com, to send an email to Campaign Official 1 at that donaldtrump.com email account, which read in part:

Hello [Campaign Official 1], [w]e are organizing a state-wide event in Florida on August, 20 to support Mr. Trump. Let us introduce ourselves first. "Being Patriotic" is a grassroots conservative online movement trying to unite people offline. . . . [W]e gained a huge lot of followers and decided to somehow help Mr. Trump get elected. You know, simple yelling on the Internet is not enough. There should be real action. We organized rallies in New York before. Now we're focusing on purple states such as Florida.

The email also identified thirteen "confirmed locations" in Florida for the rallies and requested the campaign provide "assistance in each location."

77. On or about August 18, 2016, Defendants and their co-conspirators sent money via interstate wire to another real U.S. person recruited by the ORGANIZATION, using one of their false U.S. personas, to build a cage large enough to hold an actress depicting Clinton in a prison uniform.

78. On or about August 19, 2016, a supporter of the Trump Campaign sent a message to the ORGANIZATION-controlled "March for Trump" Twitter account about a member of the Trump Campaign ("Campaign Official 2") who was involved in the campaign's Florida operations and provided Campaign Official 2's email address at the domain donaldtrump.com. On or about the same day, Defendants and their co-conspirators used the false U.S. persona joshmilton024@gmail.com account to send an email to Campaign Official 2 at that donaldtrump.com email account.

79. On or about August 19, 2016, the real "Florida for Trump" Facebook account sent another message to the false U.S. persona "Matt Skiber" account to contact a member of the Trump

Campaign (“Campaign Official 3”) involved in the campaign’s Florida operations. On or about August 20, 2016, Defendants and their co-conspirators used the “Matt Skiber” Facebook account to contact Campaign Official 3.

80. On or about August 19, 2016, Defendants and their co-conspirators used the false U.S. persona “Matt Skiber” account to write to the real U.S. person affiliated with a Texas-based grassroots organization who previously had advised the false persona to focus on “purple states like Colorado, Virginia & Florida.” Defendants and their co-conspirators told that U.S. person, “We were thinking about your recommendation to focus on purple states and this is what we’re organizing in FL.” Defendants and their co-conspirators then sent a link to the Facebook event page for the Florida rallies and asked that person to send the information to Tea Party members in Florida. The real U.S. person stated that he/she would share among his/her own social media contacts, who would pass on the information.

81. On or about August 24, 2016, Defendants and their co-conspirators updated an internal ORGANIZATION list of over 100 real U.S. persons contacted through ORGANIZATION-controlled false U.S. persona accounts and tracked to monitor recruitment efforts and requests. The list included contact information for the U.S. persons, a summary of their political views, and activities they had been asked to perform by Defendants and their co-conspirators.

82. On or about August 31, 2016, Defendants and their co-conspirators, using a U.S. persona, spoke by telephone with a real U.S. person affiliated with a grassroots group in Florida. That individual requested assistance in organizing a rally in Miami, Florida. On or about September 9, 2016, Defendants and their co-conspirators sent the group an interstate wire to pay for materials needed for the Florida rally on or about September 11, 2016.

83. On or about August 31, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for a rally they organized and scheduled in New York for September 11, 2016.

84. On or about September 9, 2016, Defendants and their co-conspirators, through a false U.S. persona, contacted the real U.S. person who had impersonated Clinton at the West Palm Beach rally. Defendants and their co-conspirators sent that U.S. person money via interstate wire as an inducement to travel from Florida to New York and to dress in costume at another rally they organized.

85. On or about September 22, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for a series of rallies they organized in Pennsylvania called “Miners for Trump” and scheduled for October 2, 2016.

All in violation of Title 18, United States Code, Section 371.

## **COUNT TWO**

### **(Conspiracy to Commit Wire Fraud and Bank Fraud)**

86. Paragraphs 1 through 7, 9 through 27, and 29 through 85 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

87. From in or around 2016 through present, in the District of Columbia and elsewhere, Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, and GLEB IGOREVICH VASILCHENKO, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit certain offenses against the United States, to wit:

- a. to knowingly, having devised and intending to devise a scheme and artifice to defraud, and to obtain money and property by means of false and fraudulent

pretenses, representations, and promises, transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purposes of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343; and

- b. to knowingly execute and attempt to execute a scheme and artifice to defraud a federally insured financial institution, and to obtain monies, funds, credits, assets, securities and other property from said financial institution by means of false and fraudulent pretenses, representations, and promises, all in violation of Title 18, United States Code, Section 1344.

**Object of the Conspiracy**

88. The conspiracy had as its object the opening of accounts under false names at U.S. financial institutions and a digital payments company in order to receive and send money into and out of the United States to support the ORGANIZATION's operations in the United States and for self-enrichment.

**Manner and Means of the Conspiracy**

89. Beginning in at least 2016, Defendants and their co-conspirators used, without lawful authority, the social security numbers, home addresses, and birth dates of real U.S. persons without their knowledge or consent. Using these means of stolen identification, Defendants and their co-conspirators opened accounts at a federally insured U.S. financial institution ("Bank 1"), including the following accounts:

Approximate Date	Account Name	Means of Identification
June 16, 2016	T.B.	Social Security Number Date of Birth
July 21, 2016	A.R.	Social Security Number Date of Birth
July 27, 2016	T.C.	Social Security Number Date of Birth
August 2, 2016	T.W.	Social Security Number Date of Birth

90. Defendants and their co-conspirators also used, without lawful authority, the social security numbers, home addresses, and birth dates of real U.S. persons to open accounts at PayPal, a digital payments company, including the following accounts:

Approximate Date	Initials of Identity Theft Victim	Means of Identification
June 16, 2016	T.B.	Social Security Number Date of Birth
July 21, 2016	A.R.	Social Security Number Date of Birth
August 2, 2016	T.W.	Social Security Number Date of Birth
November 11, 2016	J.W.	Home Address
January 18, 2017	V.S.	Social Security Number

Defendants and their co-conspirators also established other accounts at PayPal in the names of false and fictitious U.S. personas. Some personas used to register PayPal accounts were the same as the false U.S. personas used in connection with the ORGANIZATION's social media accounts.

91. Defendants and their co-conspirators purchased credit card and bank account numbers from online sellers for the unlawful purpose of evading security measures at PayPal, which used account numbers to verify a user's identity. Many of the bank account numbers purchased by Defendants

and their co-conspirators were created using the stolen identities of real U.S. persons. After purchasing the accounts, Defendants and their co-conspirators submitted these bank account numbers to PayPal.

92. On or about the dates identified below, Defendants and their co-conspirators obtained and used the following fraudulent bank account numbers for the purpose of evading PayPal's security measures:

Approximate Date	Card/Bank Account Number	Financial Institution	Email Used to Acquire Account Number
June 13, 2016	xxxxxxxx8902	Bank 2	wemakeweather@gmail.com
June 16, 2016	xxxxxxx8731	Bank 1	allforusa@yahoo.com
July 21, 2016	xxxxxxx2215	Bank 3	antwan_8@yahoo.com
August 2, 2016	xxxxxxx5707	Bank 1	xtimwaltersx@gmail.com
October 18, 2016	xxxxxxxx5792	Bank 4	unitedvetsofamerica@gmail.com
October 18, 2016	xxxxxxxx4743	Bank 4	patriototus@gmail.com
November 11, 2016	xxxxxxxx2427	Bank 4	beautifullelly@gmail.com
November 11, 2016	xxxxxxxx7587	Bank 5	staceyredneck@gmail.com
November 11, 2016	xxxxxxxx7590	Bank 5	ihatecrime1@gmail.com
November 11, 2016	xxxxxxxx1780	Bank 6	staceyredneck@gmail.com
November 11, 2016	xxxxxxxx1762	Bank 6	ihatecrime1@gmail.com
December 13, 2016	xxxxxxxx6168	Bank 6	thetaylorbrooks@aol.com
March 30, 2017	xxxxxxxx6316	Bank 3	wokeaztec@outlook.com
March 30, 2017	xxxxxxx9512	Bank 3	wokeaztec@outlook.com

93. Additionally, and in order to maintain their accounts at PayPal and elsewhere, including online cryptocurrency exchanges, Defendants and their co-conspirators purchased and obtained false identification documents, including fake U.S. driver's licenses. Some false identification documents obtained by Defendants and their co-conspirators used the stolen identities of real U.S. persons, including U.S. persons T.W. and J.W.

94. After opening the accounts at Bank 1 and PayPal, Defendants and their co-conspirators used them to receive and send money for a variety of purposes, including to pay for certain ORGANIZATION expenses. Some PayPal accounts were used to purchase advertisements on Facebook promoting ORGANIZATION-controlled social media accounts. The accounts were also used to pay other ORGANIZATION-related expenses such as buttons, flags, and banners for rallies.

95. Defendants and their co-conspirators also used the accounts to receive money from real U.S. persons in exchange for posting promotions and advertisements on the ORGANIZATION-controlled social media pages. Defendants and their co-conspirators typically charged certain U.S. merchants and U.S. social media sites between 25 and 50 U.S. dollars per post for promotional content on their popular false U.S. persona accounts, including Being Patriotic, Defend the 2nd, and Blacktivist.

All in violation of Title 18, United States Code, Section 1349.

### **COUNTS THREE THROUGH EIGHT**

#### **(Aggravated Identity Theft)**

96. Paragraphs 1 through 7, 9 through 27, and 29 through 85, and 89 through 95 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

97. On or about the dates specified below, in the District of Columbia and elsewhere,

Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, GLEB IGOREVICH VASILCHENKO, IRINA VIKTOROVNA KAVERZINA, and VLADIMIR VENKOV did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, wire fraud and bank fraud, knowing that the means of identification belonged to another real person:

Count	Approximate Date	Initials of Identity Theft Victim	Means of Identification
3	June 16, 2016	T.B.	Social Security Number Date of Birth
4	July 21, 2016	A.R.	Social Security Number Date of Birth
5	July 27, 2016	T.C.	Social Security Number Date of Birth
6	August 2, 2016	T.W.	Social Security Number Date of Birth
7	January 18, 2017	V.S.	Social Security Number
8	May 19, 2017	J.W.	Home Address Date of Birth

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

#### **FORFEITURE ALLEGATION**

98. Pursuant to Federal Rule of Criminal Procedure 32.2, notice is hereby given to Defendants that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2), and Title 28, United States Code, Section 2461(c), in the event of Defendants' convictions under Count Two of this Indictment. Upon conviction of the offense charged in Count Two, Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, and GLEB IGOREVICH VASILCHENKO

shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to the offense of conviction. Upon conviction of the offenses charged in Counts Three through Eight, Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, GLEB IGOREVICH VASILCHENKO, IRINA VIKTOROVNA KAVERZINA, and VLADIMIR VENKOV shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to the offense(s) of conviction. Notice is further given that, upon conviction, the United States intends to seek a judgment against each Defendant for a sum of money representing the property described in this paragraph, as applicable to each Defendant (to be offset by the forfeiture of any specific property).

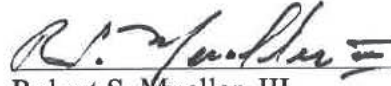
**Substitute Assets**

99. If any of the property described above as being subject to forfeiture, as a result of any act or omission of any defendant --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property that cannot be subdivided without difficulty;

it is the intent of the United States of America, pursuant to Title 18, United States Code, Section 982(b) and Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853, to seek forfeiture of any other property of said Defendant.

(18 U.S.C. §§ 981(a)(1)(C) and 982; 28 U.S.C. § 2461(c))



Robert S. Mueller, III  
Special Counsel  
U.S. Department of Justice

A TRUE BILL:

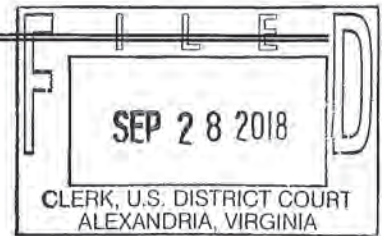


Foreperson

Date: February 16 2018

AO 91 (Rev. 11/11) Criminal Complaint

**UNDER SEAL**  
**UNITED STATES DISTRICT COURT**  
for the  
Eastern District of Virginia



United States of America  
v.

Case No. 1:18-MJ-464

ELENA ALEKSEEVNA KHUSYAYNOVA

*Defendant(s)*

**CRIMINAL COMPLAINT**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of the year 2014 until the present in the county of Alexandria in the  
Eastern District of Virginia, the defendant(s) violated:

*Code Section*

*Offense Description*

18 U.S.C. § 371

Conspiracy to defraud the United States

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Jay Prabhu; SAUSA Alex Iftimie

*Complainant's signature*

David Holt, Special Agent, FBI

*Printed name and title*

Sworn to before me and signed in my presence.

Date: 28 Sep 18

City and state: Alexandria, Virginia

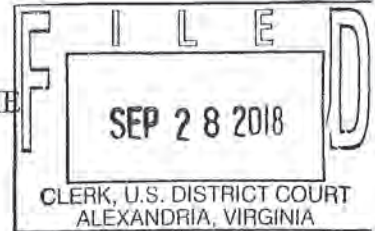
/s/

Ivan D. Davis

United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

ELENA ALEKSEEVNA KHUSYAYNOVA,

Defendant.

)  
)  
) Case No. 1:18-MJ-464  
)  
)  
) 18 U.S.C. § 371  
) (Conspiracy)  
)  
) UNDER SEAL

**AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT**

I, David Holt, being duly sworn under oath, do hereby depose and state:

**INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since August 2008. I am presently assigned to the Washington Field Office where I am responsible for investigations of foreign influence operations and other national security matters with a cyber nexus. I have also conducted national security investigations of foreign intelligence services and the targeting of critical U.S. infrastructure. As a Special Agent, I have received specialized training and instruction in the field of national security investigations and am authorized to investigate violation of laws of the United States and to execute warrants issued under the authority of the United States.

2. I am submitting this affidavit in support of a criminal complaint and arrest warrant charging the defendant, ELENA ALEKSEEVNA KHUSYAYNOVA, with Conspiracy to defraud the United States, in violation of Title 18, United States Code, Section 371.

3. The statements contained in this Affidavit are based on my experience and background as a criminal investigator, on information provided to me by other members of the

FBI and other law enforcement officers, court records and documents, business records, interviews, publicly available information, and my review of physical and documentary evidence. I have personally participated in the investigation of the offense set forth below and, as a result of my participation and review of evidence gathered in the case, I am familiar with the facts and circumstances of this investigation. Since this Affidavit is being submitted for the limited purpose of supporting a criminal complaint, I have not included every fact resulting from the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe the above-named defendant has violated Title 18, United States Code, Section 371, as set forth herein.

#### **RELEVANT STATUTES AND BACKGROUND**

4. Title 18, United States Code, Section 371, makes it a federal crime if “two or more persons conspire . . . to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy.”

5. The United States of America, through its departments and agencies, regulates the activities of foreign individuals and entities in and affecting the United States in order to prevent, disclose, and counteract improper foreign influence on U.S. elections and on the U.S. political system. U.S. law bans foreign nationals from making certain expenditures or providing things of value for the purpose of influencing federal elections. U.S. law also bars agents of any foreign entity from engaging in political activities within the United States without first registering with the Attorney General. Various federal agencies, including the U.S. Department of Justice and the Federal Election Commission, are charged with enforcing these laws.

6. The U.S. Department of Justice administers the Foreign Agent Registration Act (“FARA”), Title 22, United States Code, Section 611 *et seq.* FARA establishes a registration, reporting, and disclosure regime for agents of foreign principals (which includes foreign non-government individuals and entities) so that the U.S. government and the people of the United States are informed of the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and law. FARA requires, among other things, that persons subject to its requirements submit periodic registration statements containing truthful information about their activities and the income earned from them. Disclosure of the required information allows the federal government and the American people to evaluate the statements and activities of such persons in light of their function as foreign agents.

7. The Federal Election Commission is a federal agency that administers the Federal Election Campaign Act (“FECA”). Among other things, FECA prohibits foreign nationals from making “a contribution or donation of money or other thing of value, or to make an express or implied promise to make a contribution or donation, in connection with a Federal, State, or local election.” 52 U.S.C. § 30121(a)(1)(A). FECA also requires that individuals or entities who make certain independent expenditures in federal elections report those expenditures to the Federal Election Commission. The reporting requirements permit the Federal Election Commission to fulfill its statutory duties of providing the American public with accurate data about the financial activities of individuals and entities supporting federal candidates, and enforcing FECA’s limits and prohibitions, including the ban on foreign expenditures.

## **STATEMENT OF PROBABLE CAUSE**

### **I. Project Lakhta and Efforts to Interfere with U.S. Political System**

8. Since at least 2014, known and unknown individuals, operating as part of a broader Russian effort known as “Project Lakhta,” have engaged in political and electoral interference operations targeting populations within the Russian Federation and in various other countries, including, but not limited to, the United States, members of the European Union, and Ukraine. Since at least May 2014, Project Lakhta’s stated goal in the United States was to spread distrust towards candidates for political office and the political system in general.

9. Beginning in or around mid-2014 and continuing to the present, Project Lakhta obscured its conduct by operating through a number of Russian entities, including Internet Research Agency LLC (“IRA”), Internet Research LLC, MediaSintez LLC, GlavSet LLC, MixInfo LLC, Azimut LLC, NovInfo LLC, Nevskiy News LLC (a/k/a “NevNov”), Economy Today LLC, National News LLC, Federal News Agency LLC (a/k/a “FAN”), and International News Agency LLC (a/k/a “MAN”). These entities employed hundreds of individuals in support of Project Lakhta’s operations with an annual global budget of millions of U.S. dollars. Only some of Project Lakhta’s activities were directed at the United States.

10. Concord Management and Consulting LLC and Concord Catering (collectively “Concord”) are related Russian entities with various Russian government contracts. Concord was the primary source of funding for Project Lakhta operations. Concord controlled funding, recommended personnel, and oversaw Project Lakhta activities through reporting and interaction with the management of the various Project Lakhta entities.

11. Yevgeniy Viktorovich Prigozhin is a Russian oligarch who is closely identified with Russian President Vladimir Putin. Prigozhin began his career in the food and restaurant

business and is sometimes referred to as “Putin’s Chef.” Prigozhin controls Concord, which has been paid by the Russian government to feed school children and the military. Concord and Prigozhin spent significant funds to further the Project Lakhta operations.

12. On February 16, 2018, a grand jury in the District of Columbia returned an indictment charging thirteen Russian nationals and three Russian companies, including Prigozhin, the IRA, and Concord, with committing federal crimes while seeking to interfere with U.S. elections and political processes, including the 2016 presidential election. Indictment, *United States v. Internet Research Agency, et al.*, 1:18-CR-32 (DLF) (D.D.C. Feb. 16, 2018). Based on my training and experience, the factual allegations in that indictment provide further probable cause to believe that the above-named defendant has violated Title 18, United States Code, Section 371. That indictment is attached hereto and incorporated by reference.

## **II. ELENA ALEKSEEVNA KHUSYAYNOVA**

13. Defendant ELENA ALEKSEEVNA KHUSYAYNOVA is a resident of St. Petersburg, Russia. Since at least 2014, the defendant has been employed by various entities within Project Lakhta, including the IRA, GlavSet, and the Federal News Agency. Since approximately April 2014, she has acted as the Chief Accountant in Project Lakhta’s finance department. As detailed further herein, KHUSYAYNOVA oversaw all aspects of Project Lakhta financing. She managed the budgeting and payment of expenses associated with social media operations, web content, advertising campaigns, infrastructure, salaries, travel, office rent, furniture, and supplies, and the registration of legal entities used to further Project Lakhta activities.

14. There is probable cause to believe that, from at least 2014 to the present, KHUSYAYNOVA conspired with persons known and unknown to defraud the United States by

impairing, obstructing, and defeating the lawful functions of the U.S. Department of Justice and Federal Election Commission in administering federal requirements for disclosure of foreign involvement in certain domestic activities, in violation of Title 18, United States Code, Section 371. Among the persons with whom KHUSYAYNOVA conspired are known and unknown employees and associates of Concord and Project Lakhta entities. The Conspiracy had as its objects impairing, obstructing, and defeating the lawful governmental functions of the United States by dishonest means in order to enable Project Lakhta actors to interfere with U.S. political and electoral processes, including the 2018 U.S. elections.

### **III. Manner and Means of the Conspiracy**

15. The Conspiracy has a strategic goal, which continues to this day, to sow division and discord in the U.S. political system, including by creating social and political polarization, undermining faith in democratic institutions, and influencing U.S. elections, including the upcoming 2018 midterm election. The Conspiracy has sought to conduct what it called internally “information warfare against the United States of America”<sup>1</sup> through fictitious U.S. personas on social media platforms and other Internet-based media.

16. Members of the Conspiracy, posing as U.S. persons, operated fictitious social media personas, pages, and groups designed to attract U.S. audiences and to address divisive U.S. political and social issues or advocate for the election or electoral defeat of particular candidates. These personas, groups, and pages falsely claimed to be controlled by U.S. activists when, in fact, they were controlled by members of the Conspiracy. Over time, these accounts

---

<sup>1</sup> Throughout this affidavit, statements by members of the Conspiracy are translated or quoted exactly as they appear in the source text, including any spelling, grammatical, or factual errors.

became the Conspiracy's primary means to reach significant numbers of Americans for purposes of interfering with the U.S. political system.

17. Members of the Conspiracy made various expenditures to carry out those activities, including buying social media analytics products and services, as well as advertisements on social media, in some instances through third-party intermediaries. Members of the Conspiracy also staged and promoted political rallies inside the United States, and while posing as U.S. grassroots entities and U.S. persons, and without revealing their Russian identities and Project Lakhta affiliation, promoted or disparaged candidates and campaigns and organized rallies and counter-protests around particular socially divisive issues.

***A. KHUSYAYNOVA's Role in Project Lakhta***

18. To effectively manage such a large-scale operation, the Conspiracy was headed by a management group and organized into departments, including a design and graphics department, an analysts department, a search-engine optimization ("SEO") department, an information-technology ("IT") department, and a finance department.

19. Between April 2014 and the present, KHUSYAYNOVA, as the Chief Accountant in Project Lakhta's finance department, managed the financing of substantially all aspects of Project operations, which included media and influence activities directed at the United States, the European Union, and Ukraine, as well as the Russian Federation. In that role, she oversaw the budgets of various Project Lakhta entities, including the IRA, MediaSintez LLC, GlavSet LLC, MixInfo LLC, Azimut LLC, NovInfo LLC, Nevskiy News LLC, Economy Today LLC, National News LLC, Federal News Agency LLC, and International News Agency LLC. KHUSYAYNOVA participated in the preparation and submission of hundreds of financial vouchers, budgets, and payment requests for the various Project Lakhta entities, often putting all

company names on the same paperwork and identifying them as part of Project Lakhta.

KHUSYAYNOVA maintained Project Lakhta monthly budgets and submitted associated requests for funds to the central finance offices of Concord, which were responsible for disbursing money to Project Lakhta entities.

20. To conceal the nature of Project Lakhta activities, since at least January 2016 the Conspiracy labeled the funds paid by Concord to Project Lakhta as payments related to software support and development. Moreover, since at least January 2016, Concord distributed funds to Project Lakhta through approximately fourteen bank accounts held in the names of Concord affiliates, including Glavnaya Liniya LLC, Mercuriy LLC, Obshchepit LLC, Potentsial LLC, RSP LLC, ASP LLC, MTTs LLC, Kompleksservis LLC, SPb Kulinariya LLC, Almira LLC, Pishchevik LLC, Galant LLC, Rayteks LLC, and Standart LLC. The Conspiracy described payments from these Concord entities to Project Lakhta as being in furtherance of a series of vague contracts that obscured or falsely stated the true intended use of the funds. At various times, such payments were described as being for “providing services to collect and process materials,” “providing services in developing an exporting module for results,” and “providing services for developing a statistical processing module” (preliminary translation of Russian text).

21. At the same time, KHUSYAYNOVA kept detailed financial documents that tracked itemized Project Lakhta expenses, including efforts to promote the illegal objects of the Conspiracy in the United States. For example, the financial documents included itemized budgets that included IT expenses, social media marketing expenses, and expenses for activities in the United States and the European Union, including expenditures for activists and advertisements on social media platforms. KHUSYAYNOVA also issued and kept track of requests to Concord for funds to cover those expenses. Between at least January 2016 and July

2018, these documents were updated and provided to Concord on approximately a monthly basis. The following illustrative examples demonstrate KHUSYAYNOVA's meticulous record-keeping and management of Project Lakhta funds:

- a. In or around January 2017, KHUSYAYNOVA compiled and submitted to Concord a planned itemized budget for February 2017 for Project Lakhta totaling approximately 60 million Russian rubles (approximately \$1 million U.S. dollars).<sup>2</sup> This budget also contained a backward-looking accounting of actual expenses for calendar year 2016, which totaled approximately 720 million Russian rubles (approximately \$12 million U.S. dollars). In addition to administrative expenses, such as office rent, utility payments, and garbage disposal, the budget identified IT expenses, such as "registration of domain names" and the purchase of "proxy servers;" and social media marketing expenses, such as expenses for "purchasing posts for social networks," "[a]dvertisement on Facebook," "[a]dvertisement on VKontakte," "[a]dvertisement on Instagram," "[p]romoting news postings on social networks," and social media optimization software (such as Twidium and Novapress) (preliminary translation of Russian text). The budgets also contained a section on "USA, EU" activities, which included itemized expenditures for "Instagram," "Facebook advertisement," and "Activists" (preliminary translation of Russian text). Moreover, the budgets identified expenditures for "bloggers" and "developing accounts" on Twitter, and for the development and promotion of online videos (preliminary translation of Russian text).

---

<sup>2</sup> For the purpose of this affidavit, the approximate U.S. dollar values are based on an approximate currency conversion rate of 60 Russian rubles to 1 U.S. dollar.

- b. To cover the February 2017 expenses, KHUSYAYNOVA requested funds from Concord in two parts. KHUSYAYNOVA requested approximately 25 million Russian rubles on or about February 16, 2017, and approximately 35 million Russian rubles on March 6, 2017.
- c. In or around January 2018, KHUSYAYNOVA compiled and submitted to Concord a planned itemized budget for February 2018 totaling approximately 100 million Russian rubles (approximately \$1.7 million U.S. dollars). This budget also contained a backward-looking accounting of actual expenses for calendar year 2017, which totaled approximately 733 million Russian rubles (approximately \$12.2 million U.S. dollars). The budget contained, among other things, all of the categories of itemized expenditures identified in subparagraph a, above.
- d. To cover substantial portions of the February 2018 expenses, KHUSYAYNOVA requested funds from Concord in at least six parts. KHUSYAYNOVA requested approximately 20 million Russian rubles on or about February 7, 2018, approximately 10 million Russian rubles on or about February 7, 2018, approximately 15 million Russian rubles on or about February 16, 2018, approximately 3 million Russian rubles on or about February 21, 2018, approximately 5 million Russian rubles on or about February 28, 2018, and approximately 31 million Russian rubles on or about March 6, 2018.
- e. In or around March 2018, KHUSYAYNOVA compiled and submitted to Concord a monthly budget for April 2018 for Project Lakhta that exceeded 107 million

Russian rubles (over \$1.75 million U.S. dollars). The budget contained, among other things, all of the itemized expenditures identified in subparagraph a, above.

- f. To cover substantial portions of the April 2018 expenses, KHUSYAYNOVA requested funds from Concord in at least two parts. KHUSYAYNOVA requested approximately 32 million Russian rubles on or about April 6, 2018, and approximately 21 million Russian rubles on or about May 8, 2018.
- g. In or around April 2018, KHUSYAYNOVA compiled and submitted to Concord a monthly budget for May 2018 for Project Lakhta that exceeded 111 million Russian rubles (over \$1.86 million U.S. dollars). The budget contained, among other things, all of the categories of itemized expenditures identified in subparagraph a, above.
- h. To cover substantial portions of the May 2018 expenses, she requested funds from Concord in at least three parts. She requested approximately 5 million Russian rubles on or about May 8, 2018, approximately 31 million Russian rubles on or about May 10, 2018, and approximately 35 million Russian rubles on or about June 9, 2018.
- i. On or about June 1, 2018, KHUSYAYNOVA compiled and submitted to Concord a monthly budget for June 2018 for Project Lakhta that exceeded 114 million Russian rubles (over \$1.9 million U.S. dollars). The budget contained, among other things, all of the categories of itemized expenditures identified in subparagraph a, above.
- j. To cover substantial portions of the June 2018 expenses, KHUSYAYNOVA requested funds from Concord in three parts. KHUSYAYNOVA requested

approximately 29 million Russian rubles on or about June 1, 2018, approximately 29 million Russian rubles on or about June 4, 2018, and approximately 36 million Russian rubles on July 10, 2018.

22. Between in or around January 2016 and in or around June 2018, Project Lakhta's proposed operating budget totaled more than 2 billion Russian rubles (over \$35 million U.S. dollars). Just between in or around January 2018 and in or around June 2018, Project Lakhta's proposed operating budget totaled more than 650 million Russian rubles (over \$10 million U.S. dollars).

23. KHUSYAYNOVA also monitored the Project Lakhta budget to ensure that expected payments from Concord were received. For example, on or about November 15, 2017, KHUSYAYNOVA contacted Concord to inform them that she had not received a payment from Almira LLC for certain Project Lakhta companies, and that she was urgently waiting for the payment. Similarly, on or about April 11, 2018, KHUSYAYNOVA confirmed to Concord that she had received payment for a portion of the March 2018 budget for Project Lakhta but was waiting for the remaining payment. On or about April 12, 2018, a Concord employee informed KHUSYAYNOVA that the remaining payment would be forthcoming.

24. Starting at least in or around 2015, the Conspiracy began to purchase advertisements on online social media sites to promote events and social media groups it controlled. These expenditures were included in the budgets that KHUSYAYNOVA submitted to Concord. For example, between approximately January 2018 and June 2018, KHUSYAYNOVA compiled and submitted to Concord expenditures of over 3.7 million Russian rubles (over \$60,000 U.S. dollars) for advertisements on Facebook and over 385,000 Russian rubles (over \$6,000 U.S. dollars) for advertisements on Instagram. Over that same timeframe,

the budget also included expenditures of over 1,100,000 Russian rubles (over \$18,000 U.S. dollars) for “bloggers” and “[d]eveloping accounts” on Twitter (preliminary translation of Russian text). Additionally, the budget included expenditures for “[r]enting software for social networks,” including payments for services to manage Twitter posts and generate additional followers (preliminary translation of Russian text).

***B. Targeted Messaging to Sow Social and Political Discord***

25. Between in or around December 2016 and in or around May 2018, as part of the Conspiracy’s effort to sow discord in the U.S. political system, members of the Conspiracy used social media and other internet platforms to inflame passions on a wide variety of topics, including immigration, gun control and the Second Amendment, the Confederate flag, race relations, LGBT issues, the Women’s March, and the NFL national anthem debate. Members of the Conspiracy took advantage of specific events in the United States to anchor their themes, including the shootings of church members in Charleston, South Carolina, and concert attendees in Las Vegas, Nevada; the Charlottesville “Unite the Right” rally and associated violence; police shootings of African-American men; as well as the personnel and policy decisions of the current U.S. administration.

26. Members of the Conspiracy were directed to create “political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements.” The Conspiracy also sought, in the words of one member of the Conspiracy, to “effectively aggravate the conflict between minorities and the rest of the population.”

27. The Conspirators’ activities did not exclusively adopt one ideological viewpoint; they wrote on topics from varied and sometimes opposing perspectives. Members of the

Conspiracy also developed strategies and guidance to target audiences with conservative and liberal viewpoints, as well as particular social groups. For example, a member of the Conspiracy advised in or around October 2017 that “if you write posts in a liberal group, . . . you must not use Breitbart titles. On the contrary, if you write posts in a conservative group, do not use Washington Post or BuzzFeed’s titles.” Using the example of individuals of color who are also members of the lesbian, gay, bisexual, and transgender (“LGBT”) community, the member of the Conspiracy offered the following guidance on how to target the group:

Colored LGBT are less sophisticated than white; therefore, complicated phrases and messages do not work. Be careful dealing with racial content. Just like ordinary Blacks, Latinos, and Native Americans, colored LGBT people are very sensitive towards *#whiteprivilege* and they react to posts and pictures that favor white people. . . . Unlike with conservatives, infographics works well among LGBT and their liberal allies, and it does work very well. However, the content must be simple to understand consisting of short text in large font and a colorful picture. (Preliminary translation of Russian text.)

Members of the Conspiracy also sought to target the timing of their posts to attract the widest possible viewership. The same member of the Conspiracy referenced above offered the following guidance on how to overcome the time difference between Russia and the United States:

Posting can be problematic due to time difference, but if you make your re-posts in the morning St. Petersburg time, it works well with liberals – LGBT groups are often active at night. Also, the conservative can view your re-post when they wake up in the morning if you post it before you leave in the evening St. Petersburg time. (Preliminary translation of Russian text.)

28. Members of the Conspiracy also developed detailed analysis of timely news articles and guidance for how to describe the articles in social media posts in order to promote the objectives of the Conspiracy. For example, in or around early August 2017, one or more members of the Conspiracy working under the guise of the Facebook group “Secured Borders”

analyzed a large quantity of U.S. news articles, summarized the substance of the articles, and outlined ways for the conspiracy to promote them. Specifically, one or more members of the Conspiracy described each article and categorized its theme, provided a strategic response with a particular focus on how to target U.S. audiences, and then noted approval to use the strategic response. The strategic response was referred to as “Tasking Specifics,” which appeared to include an assignment to certain members of the Conspiracy to disseminate the message on social media platforms.

- a. Citing an online news article titled “McCain Says Thinking a Wall Will Stop Illegal Immigration is ‘Crazy,’” from on or about August 5, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Brand McCain as an old geezer who has lost it and who long ago belonged in a home for the elderly. Emphasize that John McCain’s pathological hatred towards Donald Trump and towards all his initiatives crosses all reasonable borders and limits. State that dishonorable scoundrels, such as McCain, immediately aim to destroy all the conservative voters’ hopes as soon as Trump tries to fulfill his election promises and tries to protect the American interests. (Preliminary translation of Russian text.)

- b. Citing an online news article titled “Paul Ryan Opposes Trump’s Immigration Cuts, Wants Struggling American Workers to Stay Poor,” from on or about August 5, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Brand Paul Ryan a complete and absolute nobody incapable of any decisiveness. Emphasize that while serving as Speaker, this two-faced loudmouth has not accomplished anything good for America or for American citizens. State that the only way to get rid of Ryan from Congress, provided he wins in the 2018 primaries, is to vote in favor of Randy Brice, an American veteran and an iron worker and a Democrat. (Preliminary translation of Russian text.)

- c. Citing an online news article titled "11 California Counties Might have More Registered Voters Than Eligible," from on or about August 6, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

In the California voter registration rolls, there are more registrants than there are residents. This is the time for American conservatives to sound the alarm before the elections turn the Constitution into a mockery and a celebration of lawlessness. Emphasize that previous falsifications during the U.S. elections used to be perceived as a myth; today they became a reality with a threatening force and are perceived accordingly. Emphasize that all illegal voters must be kept away from the ballot boxes at distances "beyond artillery firing range." There is an urgent need to introduce voter IDs for all the states, above all in the blue (liberal and undecided) states. Remind that the majority of the "blue states" have no VOTER IDs, which suggests that large-scale falsifications are bound to be happening there. State in the end that the Democrats in the coming election will surely attempt to falsify the results. (Preliminary translation of Russian text.)

- d. Citing an online news article titled "Savage: Civil War if Trump Taken Down," from on or about August 6, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Forcefully support Michael Savage's point of view with competence and honesty. Savage made it clear that any attempt to remove Trump is a direct path to a civil war in the United States. Name those who oppose the president and those who impede his efforts to implement his pre-election promises. Focus on the fact that the Anti-Trump Republicans: a) drag their feet with regard to financing the construction of the border wall; b) are not lowering taxes; c) slander Trump and harm his reputation (bring up McCain); d) do not want to cancel Obamacare; e) are not in a hurry to adopt laws that oppose the refugees coming from Middle Eastern countries entering this country. Summarize that in case Republicans will not stop acting as traitors, they will bring upon themselves forces of civil retribution during the 2018 elections. (Preliminary translation of Russian text.)

- e. Citing an online news article titled “Trump: No Welfare To Migrants For Grants For First 5 Years” from on or about August 6, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Fully support Donald Trump and express the hope that this time around Congress will be forced to act as the president says it should. Emphasize that if Congress continues to act like the Colonial British government did before the War of Independence, this will call for another revolution. Summarize that Trump once again proved that he stands for protecting the interests of the United States of America. (Preliminary translation of Russian text.)

- f. Citing an online news article titled “The 8 Dirtiest Scandals of Robert Mueller No One Is Talking About,” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Special prosecutor Mueller is a puppet of the establishment. List scandals that took place when Mueller headed the FBI. Direct attention to the listed examples. State the following: It is a fact that the Special Prosecutor who leads the investigation against Trump represents the establishment: a politician with proven connections to the U.S. Democratic Party who says things that should either remove him from his position or disband the entire investigation commission. Summarize with a statement that Mueller is a very dependent and highly politicized figure; therefore, there will be no honest and open results from the investigation. Emphasize that the work of this commission is damaging to the country and is aimed to declare impeachment of Trump. Emphasize that it cannot be allowed, no matter what. (Preliminary translation of Russian text.)

- g. Citing an online news article titled “CNN’s Pro-Jeb! Republican: Trump White House Like a ‘Brothel,’” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

CNN commentator “RINO” likened the Trump administration to a “brothel.” Mass News Media Criticism! Accuse CNN of yet another lie. State that during past elections, namely, this mainstream media, which supported Hillary Clinton’s candidacy

for U. S. President almost 100%, disseminated fake news, insulting statements, and lies about Donald Trump and his supporters. This continues now. This is precisely why such news sources as the New York Times, Washington Post, CNN, CBS, Time, and Huffington Post must not be taken seriously, for they are the main propaganda channels that are screwing with the heads of American citizens. Remind readers that each of the above-mentioned media resources supported Hillary Clinton and received funds from her election fund. They produced fake social study research results at polls predicting a Clinton win with a 10-15% lead over Trump and tried hard to insult and discredit Trump. Summarize with a statement that CNN long ago lost its reputation as a trusted source and that its reputation is still declining. (Preliminary translation of Russian text.)

- h. Citing an online news article titled “Pro-Amnesty Sen. Marco Rubio: Trump’s Immigration Bill Will Not Pass the Senate,” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

VERY IMPORTANT! We expose Marco Rubio as a fake conservative who is a traitor to Republican values and who in his soul despises the American Constitution and civil liberties. Remind that Rubio is the protégé of the preposterous Jeb Bush, who is a disgrace to the conservative movement. State that victims of violence committed by illegals and the relatives of the victims hate Marco Rubio completely and wholeheartedly. In other words, Rubio is a liberal who penetrated the Republican Party for the purpose undermining it from the inside. Summarize in a statement that voting for Rubio during the Senate elections is practically the same as voting for Hillary Clinton. (Preliminary translation of Russian text.)

- i. Citing an online news article titled “Sanctuary City Objects to Arrest of Accused Illegal Alien Child Molester,” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Characterize the position of Californian sanctuary cities along with the position of the entire California administration as absolutely and completely treacherous and disgusting. Stress that protecting an illegal rapist who raped an American child is the peak of

wickedness and hypocrisy. Summarize in a statement that “sanctuary city” politicians should surrender their American citizenship, for they behave as true enemies of the United States of America. (Preliminary translation of Russian text.)

- j. Citing an online news article titled “Maryland City Mulling Over Idea to Let Illegal Immigrants Vote” from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

Stress that the leadership in sanctuary cities has lost all connection with reality and is trying to provide criminals who illegally crossed the U.S. borders with voting rights that are available only to the citizens of the United States. Summarize in a statement that the leaders of sanctuary cities are people without conscience and without any respect for the American Constitution. (Preliminary translation of Russian text.)

- k. Citing an online news article titled “Dobbs Slams McConnell, Says It’s Time to ‘Ditch Mitch,’” from on or about August 8, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

It’s time for Mitch McConnell (leader of the Senate Republicans) to retire. Show solid support for the news anchor. Emphasize that McConnell exhausted himself as a politician. State that Mitch McConnell, like many other Republican senators, behaves as a renegade and a vile liberal. McConnell has done nothing to fulfill Trump’s and other Republicans’ election promises. Remind that McConnell is a friend of Joe Biden, who has no political principles. Emphasize that boycotting the conservative agenda is the most inadequate and treacherous behavior possible in the given situation. Summarize in a statement that people did not vote for the Republicans in 2014 and in 2016 so that today they would do the same things that Democrats usually busy themselves with. (Preliminary translation of Russian text.)

***C. Use of Specific U.S. Fake Personas***

29. Since at least in or around 2015, the Conspiracy used social media platforms to create thousands of social media and email accounts that appeared to be operated by U.S. persons and used them to create and amplify divisive social and political content targeting a U.S.

audience. These accounts were also used to advocate for the election or electoral defeat of particular candidates in the 2016 and 2018 U.S. elections, to post derogatory information about a number of candidates, and, on occasion, to promote political donations against particular candidates.

30. In or around May 2015, the Conspiracy created a Facebook account registered under the false U.S. persona "Helen Christopherson." On her Facebook page, "Helen Christopherson" purported to be a resident of New York City and identified her hometown as Charleston, South Carolina. Between in or around March 2016 and in or around July 2017, while concealing its true identity, location, and purpose, the Conspiracy used the false U.S. persona "Helen Christopherson" to contact individuals and groups in the United States to promote protests, rallies, and marches, including by funding advertising, flyers, and rally supplies. Specific examples of this account's activities, as well as the activities of other accounts described in this subsection, are contained in the Overt Acts section below.

31. In or around June 2015, the Conspiracy created a Facebook account registered under the false U.S. persona "Bertha Malone." On her Facebook page, "Bertha Malone" purported to be a resident of New York City, identified her hometown as New York City, and stated that she had attended a university in New York City. In or around January 2016, the Conspiracy used the "Bertha Malone" Facebook account to create a Facebook page for a group called "Stop A.I.," which is an abbreviation for "Stop All Invaders." Between in or around December 2016 and in or around August 2017, while concealing its true identity, location, and purpose, the Conspiracy used the "Bertha Malone" Facebook account to create over 400 posts on Facebook containing inflammatory political and social content focused primarily on immigration and Islam. Between on or about July 17, 2017, and on or about July 23, 2017, alone, the content

on the “Stop A.I.” Facebook page reached approximately 1,385,795 individuals and approximately 130,851 individuals purposefully engaged with the Facebook page. In total, by on or about July 23, 2017, the Facebook page received approximately 194,221 total page likes.

32. The Conspiracy also used the “Bertha Malone” Facebook account, while concealing its true identity, location, and purpose, to solicit at least one person presumed to be located in the United States to assist with Project Lakhta’s social media activities in or around July 2017, such as by posting and managing content on the “Stop A.I.” Facebook page. Moreover, the Conspiracy used the “Stop A.I.” Facebook page to accept money from individuals to post ads and other content on the Facebook group’s page.

33. In or around June 2016, the Conspiracy created a Twitter account that went by various names, including “@UsaUsafortrump,” “@USAForDTrump,” “@TrumpWithUSA,” “@TrumpMov,” “@POTUSADJT,” “@imdeplorable201,” “@swampdrainer659,” “@maga2017trump,” and “@TXCowboysRawk.” Most recently, the Twitter account went by the name “@CovfefeNationUS.” Between in or around November 2017 and in or around December 2017, while concealing its true identity, location, and purpose, the Conspiracy used the Twitter account “@CovfefeNationUS” to post or repost over 23,000 messages.

34. In or around September 2016, the Conspiracy created a Facebook account registered under the false U.S. persona “Rachell Edison” and an associated Facebook page for a group called “Defend the 2nd.” Between in or around December 2016 and in or around May 2017, while concealing its true identity, location, and purpose, the Conspiracy used the “Rachell Edison” Facebook account to create over 700 posts on Facebook containing inflammatory political and social content primarily focused on gun control and the Second Amendment.

35. In or around March 2017, the Conspiracy created the Twitter account “@wokeluisa” registered under the false U.S. persona “Luisa Haynes.” Between in or around March 2017 and in or around March 2018, while concealing its true identity, location, and purpose, the Conspiracy used the Twitter account “@wokeluisa” to post over 2,000 Tweets on topics such as the 2018 midterm election, the disenfranchisement of African-American voters, the NFL national anthem debate, the current U.S. administration, and the U.S. President’s family. By in or around March 2018, the Twitter account amassed over 55,000 followers.

36. In or around September 2017, the Conspiracy created several Twitter accounts that it used to create and amplify content that would resonate with either liberal or conservative audiences. For example, on or about September 4, 2017, one or more members of the Conspiracy created the Twitter accounts “@JohnCopper16,” “@Amconvoice,” and “@TheTrainGuy13.” Members of the Conspiracy used these accounts to post messages on controversial social and political topics using a perspective that they believed would resonate with a conservative audience in the United States. Similarly, one or more members of the Conspiracy created the Twitter account “@KaniJJackson” on or about September 5, 2017, and the Twitter account “@JemiSHaaaZzz” on or about September 6, 2017, and used these accounts to post on many of the same controversial social and political topics from a perspective that they believed would resonate with a liberal audience in the United States. Between in or around September 2017 and in or around May 2018, while concealing its true identity, location, and purpose, the Conspiracy used these Twitter accounts to post thousands of Tweets, on topics including, but not limited to, the 2018 midterm election, gun rights, the net neutrality debate, negotiations with North Korea, and the personnel and policy decisions of the current U.S. administration. In some cases, these accounts attracted significant numbers of followers. For

example, by in or around May 2018, the Twitter account “@KaniJJackson” had amassed over 33,000 followers.

#### IV. Overt Acts

37. Between in or around December 2016 and in or around May 2018, in the Eastern District of Virginia and elsewhere, while concealing its true identity, location, and purpose, the Conspiracy committed the following overt acts involving U.S. social media platforms in furtherance of the Conspiracy and to effect its illegal objects:

38. On or about December 5, 2016, a member of the Conspiracy used the “Rachell Edison” Facebook account to post the following image on Facebook, accompanied by the comment “Whatever happens, blacks are innocent. Whatever happens, it’s all guns and cops. Whatever happens, it’s all racists and homophobes. MainStream Media...”:



39. On or about April 28, 2017, a member of the Conspiracy used the “Rachell Edison” Facebook account to post the following image on Facebook:



The image was accompanied by the following comment advocating political activities:

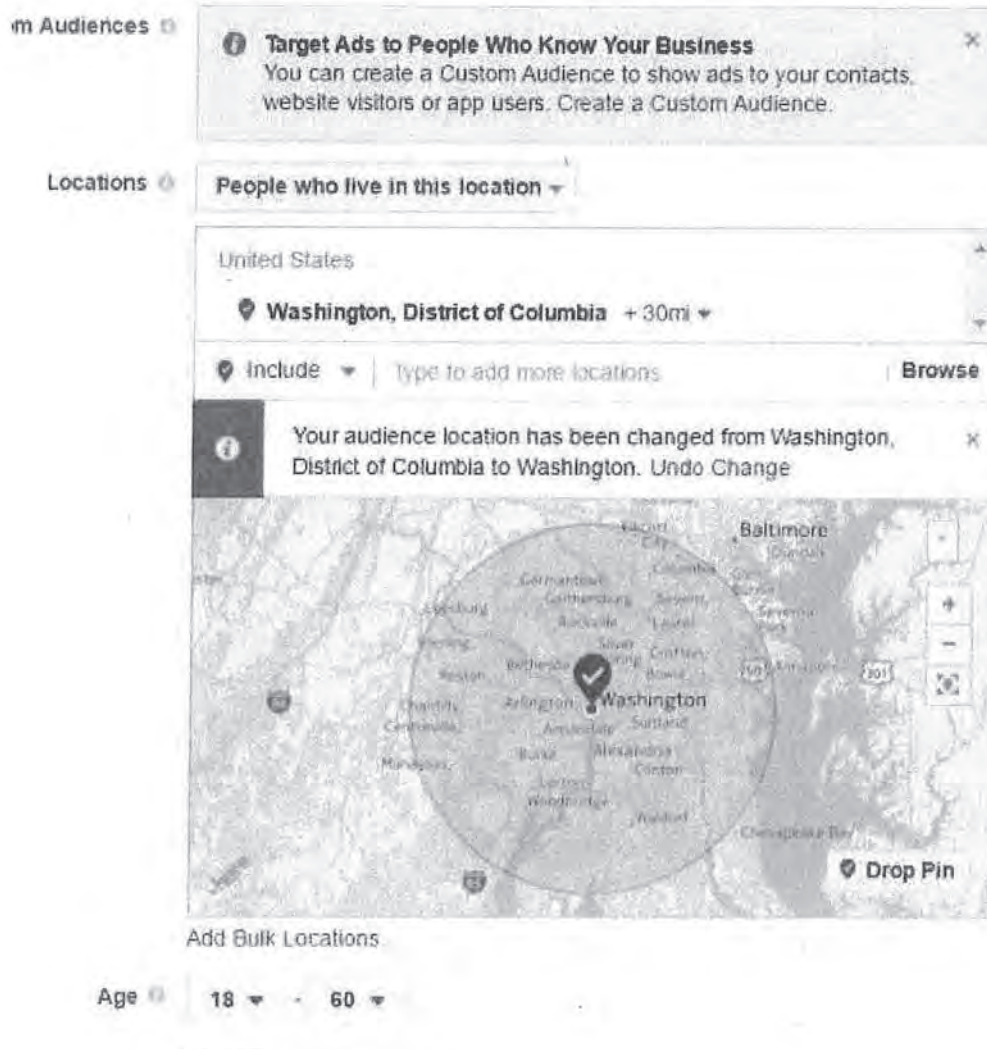
Gun rights backers need to make sure that election victories translate into action on Capitol Hill and expanded support in the states, the National Rifle Association’s legislative chief said Thursday, a day ahead of President Trump’s speech at the NRA’s annual convention. And he is absolutely right. Now it is the time for us to demand our rights. With current, administration it is possible to defend our right to bear arms. I think next 4 years will be great for all Americans, and for gun lovers especially! But we must stand for our rights! And in the end, I believe, we will win!

40. On or about July 1, 2017, a member of the Conspiracy used the “Helen Christopherson” Facebook account to contact the Facebook accounts for three real U.S. organizations (hereinafter U.S. Organizations 1, 2, and 3) to inquire about collaborating with

these groups on an anti-President Trump “flash mob” at the White House, which was already being organized by the groups for July 4, 2017. The organizers had described the event as “inviting resistance activists, show tune lovers, and karaoke fans to come join us on Independence Day, sing a song of freedom, and demand Trump’s impeachment.”

41. On or about July 2, 2017, a member of the Conspiracy used the “Helen Christopherson” Facebook account to contact U.S. Organization 1 and a U.S. person affiliated with the organization, U.S. Person 1, and inform them that “I got some cash on my Facebook ad account so we can promote it for 2 days,” adding “I got like \$80 on my ad account so we can reach like 10000 people in DC or so. That would be Massive!”

42. On or about July 2, 2017, a member of the Conspiracy used the “Helen Christopherson” Facebook account to send U.S. Organization 1 a proposal to purchase advertising targeting individuals within 30 miles of Washington, DC, including significant portions of the Eastern District of Virginia, as depicted below:



The proposed advertisements had an estimated reach of 29,000 to 58,000 individuals. Subsequently, U.S. Organization 1 agreed to make the “Helen Christopherson” Facebook account a co-organizer of the event on Facebook.

43. On or about July 4, 2017, a member of the Conspiracy used the "Bertha Malone" Facebook account to engage in the following conversation with U.S. Person 2 about U.S. Person 2 assisting with posting content and managing the "Stop A.I." Facebook page, which members of the Conspiracy controlled:

Malone: Hey girl! How u doin? still got free time on ya hands?  
So...remember u wanted to help me with that page i'm workng  
on? It's a little bit unorthodox, but nwm that. Content is not of  
my choosing. So what tell ya? Help a sister out?

U.S. Person 2: Hi! Let me think bout 4 a sec.  
what's the name of the page again?

Malone: <https://www.facebook.com/StopAllInvaders/>

...

Malone: Nothin muh, [U.S. Person 2]. Just general scannin, answer  
subscribers now and then and mb post something (i'll be sending  
content to u directly)

Malone: nwm the posts lol

Malone: just business

Malone: makes ratinging for clients, that's what i know.

Malone: ratings\*

Malone: u know how rednecks are

Malone: so here's the deal. I give u admin rights, u check the page when  
i'm not around and basically do some stuff i tell u to :D

...

U.S. Person 2: You know I can't let my sis down

U.S. Person 2: so I'm in

...

U.S. Person 2: but please tell me I'm not going to jail for this

...

Malone: jeez why would u

Malone: just page lol

Malone: i'll vouch fou 4 mb u get some money out that even

...

U.S. Person 2: i trust you

44. On or about July 28, 2017, a member of the Conspiracy used the “Bertha Malone” Facebook account to post the following image on Facebook:



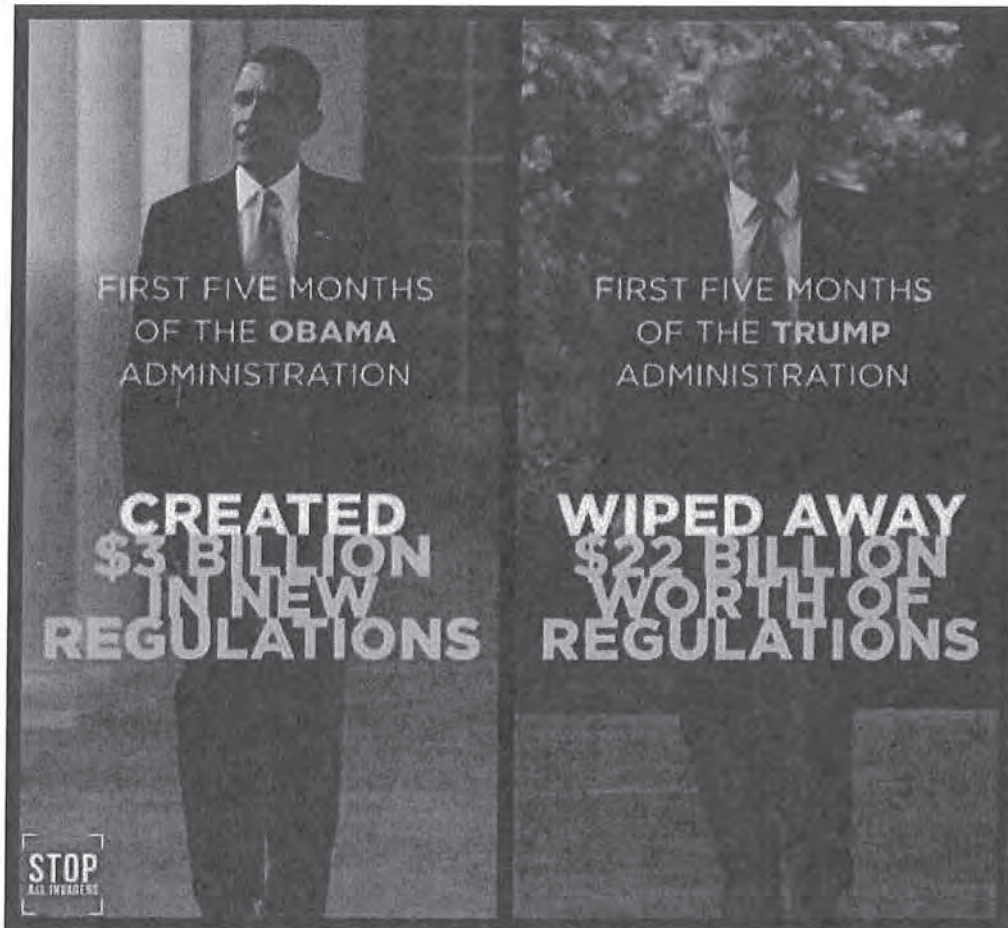
The image was accompanied by the following comment:

Instead this stupid witch hunt on Trump, media should investigate this traitor and his plan to Islamize our country. If you are true enemy of America, take a good look at Barack Hussein Obama and Muslim government officials appointed by him.

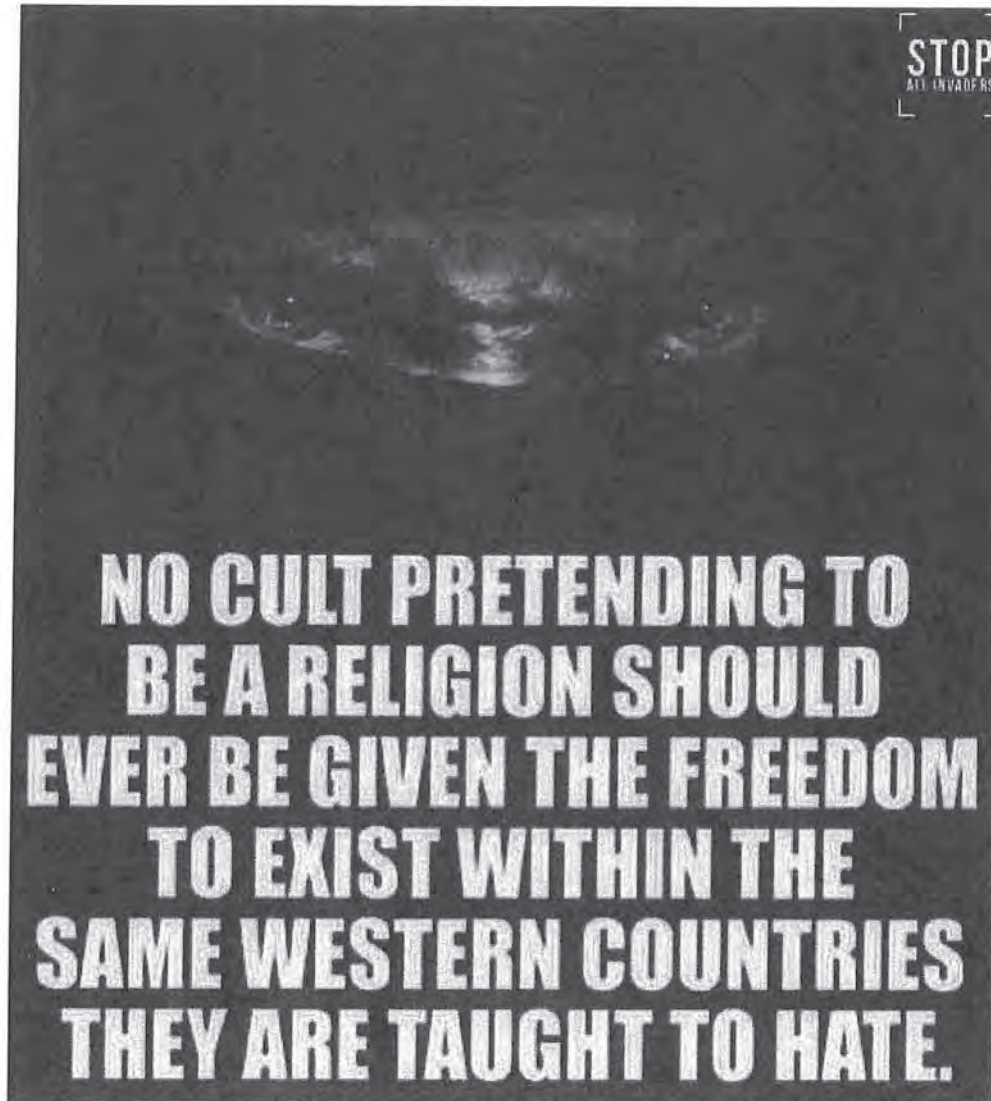
45. On or about July 31, 2017, a member of the Conspiracy used the “Bertha Malone” Facebook account to post the following image on Facebook, with the comment “Stop separating families! Deport them all, including their anchor babies! And spend saved money on Americans who really need it, for example our homeless Vets”:



46. On or about July 31, 2017, a member of the Conspiracy used the “Bertha Malone” Facebook account to post the following image on Facebook, with the comment “Feel the difference!”:



47. On or about August 1, 2017, a member of the Conspiracy used the “Bertha Malone” Facebook account to post the following image on Facebook, with the comment “Damn right! And we all know which cult we need to kick out of America...”:



The post generated approximately 104 comments between on or around August 1, 2017, and on or around August 2, 2017.

48. On or about December 10, 2017, a member of the Conspiracy used the Twitter account “@CovfefeNationUS” to repost a Tweet encouraging readers to donate to a political action committee aiming to unseat Democratic Senators and Representatives in the 2018 midterm election:

Tell us who you want to defeat! Donate \$1.00 to defeat @daveloebsack  
Donate \$2.00 to defeat @SenatorBaldwin Donate \$3.00 to defeat  
@clairecmc Donate \$4.00 to defeat @NancyPelosi Donate \$5.00 to defeat  
@RepMaxineWaters Donate \$6.00 to defeat @SenWarren

The Tweet included a link to the donation website of a political action committee.

49. On or about December 12, 2017, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the 2017 special election in Alabama:

Dear Alabama, You have a choice today. Doug Jones put the KKK in prison for murdering 4 young black girls. Roy Moore wants to sleep with your teenage daughters. This isn't hard. #AlabamaSenate

50. On or about December 12, 2017, a member of the Conspiracy used the Twitter account “@JohnCopper16” to post a Tweet about the 2017 special election in Alabama:

People living in Alabama have different values than people living in NYC. They will vote for someone who represents them, for someone who they can trust. Not you. Dear Alabama, vote for Roy Moore.

51. On or about December 16, 2017, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the Special Counsel’s Office’s investigation:

If Trump fires Robert Mueller, we have to take to the streets in protest. Our democracy is at stake.

52. On or about December 17, 2017, a member of the Conspiracy used the Twitter account “@Amconvoice” to repost a Tweet about the Special Counsel’s Office’s investigation:

Liberals : If Trump fire/removes Mueller, we will take to the streets/protest. (DNC must have sent that talking point out today. Everyone using same line) Why would Trump need to remove/fire Mueller. Mueller is doing fine job destroying himself. Keep the implosion coming Mueller.

53. On or about January 19, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the government shutdown of 2018:


Who ended DACA? Who put off funding CHIP for 4 months? Who rejected a deal to restore DACA? It's not #SchumerShutdown. It's #GOPShutdown.

54. On or about January 20, 2018, a member of the Conspiracy used the Twitter account “@JohnCopper16” to repost a Tweet about the government shutdown of 2018:

Anyone who believes that President Trump is responsible for the #shutdown2018 is either an outright liar or horribly ignorant. #SchumerShutdown for illegals. #DemocratShutdown #DemocratLosers #DemocratsDefundMilitary #AlternativeFacts

55. On or about January 26, 2018, a member of the Conspiracy used the Twitter account “@JemiSHaaaZzz” to repost a Tweet about a Senate vote on reproductive health issues, referencing the telephone number of the U.S. Capitol switchboard:



Republicans have scheduled a vote Monday on legislation that would ban some women's health care choices 

We can't turn back the clock on women's reproductive health. Call your Senators now and tell them to vote NO: (202) 224-3121.

56. On or about February 8, 2018, a member of the Conspiracy used the Twitter account “@Amconvoice” to post a Tweet about the 2018 U.S. midterm election:

The only way the Democrats can win 101 GOP seats is to cheat like they always do with illegals & dead voters.

57. On or about February 15, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the Parkland, Florida, school shooting and the 2018 U.S. midterm election:

Reminder: the same GOP that is offering thoughts and prayers today are the same ones that voted to allow loosening gun laws for the mentally ill last February. If you're outraged today, VOTE THEM OUT IN 2018.  
#guncontrol #Parkland

58. On or about February 16, 2018, a member of the Conspiracy used the Twitter account “@JemiSHaaaZzz” to repost a Tweet about the Special Counsel’s Office’s indictment of Russian companies and nationals who sought to interfere with U.S. elections and political processes:

Dear @realDonaldTrump: The DOJ indicted 13 Russian nationals at the Internet Research Agency for violating federal criminal law to help your campaign and hurt other campaigns. Still think this Russia thing is a hoax and a witch hunt? Because a lot of witches just got indicted.

59. On or about February 16, 2018, a member of the Conspiracy used the Twitter account “@JohnCopper16” to post two Tweets about the Special Counsel’s Office’s indictment:

Russians indicted today: 13 Illegal immigrants crossing Mexican border indicted today: 0 Anyway, I hope that all those Internet Research Agency f\*ckers will be sent to gitmo.

We didn't vote for Trump because of a couple of hashtags shilled by the Russians. We voted for Trump because he convinced us to vote for Trump. And we are ready to vote for Trump again in 2020!

60. On or about February 19, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post a Tweet about the 2018 midterm election:

Midterms are in 261 days, use this time to: - Promote your candidate on social media - Volunteer for a campaign - Donate to a campaign - Register to vote - Help others to register to vote - Spread the word We have only 261 days to guarantee survival of democracy. Get to work!

61. On or about February 27, 2018, a member of the Conspiracy used the Twitter account “@JohnCopper16” to post the following Tweet about the 2018 midterm election:

Dem 2018 platform: - We want women raped by the jihadists - We want children killed - We want higher gas prices - We want more illegal aliens - We want more Mexican drugs And they are wondering why @realDonaldTrump became the President...

62. On or about March 9, 2018, a member of the Conspiracy used the Twitter account “@JohnCopper16” to post the following two Tweets about the summit between President Trump and North Korean President Kim Jong Un:

WOW! Donald Trump is going to meet Kim Jong Un to discuss denuclearization of North Korea, If Trump gets North Korea to denuclearize its game over for the Democrats! That would be monumental!

RETWEET if you think that Donald Trump deserves a Nobel Peace Prize for resolving the North Korean crisis!

63. On or about March 9, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to post the following two Tweets about the summit between President Trump and North Korean President Kim Jong Un:

Trump says he will meet with Kim Jong Un in May. But he might not even be president by then. Mueller is coming!

The same people who criticized Barack Obama for signing the Iran Nuclear deal are already praising Trump for his promise to meet with Kim Jong Un and talk about denuclearization.

64. On or about March 14, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to post several Tweets regarding the Pennsylvania special election on March 13, 2018, for a House of Representatives seat:

Enthusiastically watching #PA18 turn blue

Lamb up by only 703 votes... EVERY. VOTE. COUNTS. #PA18

We need to flip about 20 seats to regain control of the House! 19 after tonight! #PA18

Tonight's results are a message regardless of the outcome: D voters are motivated! Blue Wave coming! #PA18

65. On or about March 14, 2018, a member of the Conspiracy used the Twitter account "@TheTrainGuy13" to repost a Tweet about voter fraud:



66. On or about March 18, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to post the following Tweet about election fraud:

Fun fact: the last time a new Republican president was elected without electoral fraud was in 1988

67. On or about March 18, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to repost the following Tweet:

Just a reminder that: - Majority black Flint, Michigan still has drinking water that will give you brain damage if consumed. - Republicans are still trying to keep black people from voting. - A terrorist has been targeting black families for assassination in Austin, Texas.

68. On or about March 19, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to post the following Tweets about an explosion in Austin, Texas:

Trump will tweet NOTHING about yet another explosion in Austin b/c all of the victims have been black and hispanic. Mark my words

Another explosion in southwest Austin, Texas! Why these bombings ain't a bigger story? Oh yes... all of the victims have been Black and Hispanic #AustinBombings

69. On or about March 19, 2018, a member of the Conspiracy used the Twitter account “@wokeluisa” to post the following Tweet about the 2018 midterm election:

Make sure to pre-register to vote if you are 16 y.o. or older. Don't just sit back, do something about everything that's going on because November 6, 2018 is the date that 33 senate seats, 435 seats in the House of Representatives and 36 governorships will be up for re-election.

70. On or about March 22, 2018, a member of the Conspiracy used the Twitter account “@johncopper16” to post the following Tweet about the 2018 midterm election:

Just a friendly reminder to get involved in the 2018 Midterms. They are motivated They hate you They hate your morals They hate your 1A and 2A rights They hate the Police They hate the Military They hate YOUR President

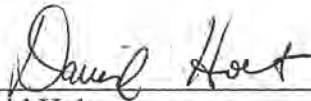
71. On or about May 17, 2018, a member of the Conspiracy used the Twitter account “@KaniJJackson” to repost two Tweets about a U.S. Senate vote on Net Neutrality:

Ted Cruz voted to repeal #NetNeutrality. Let’s save it and repeal him instead.

Here’s the list of GOP senators who broke party lines and voted to save #NetNeutrality: Susan Collins John N Kennedy Lisa Murkowski Thank you!

**CONCLUSION**

72. Based on the foregoing, and on my training, experience, and participation in this and other investigations, I submit there is probable cause to believe that, from at least 2014 to the present, ELENA ALEKSEEVNA KHUSYAYNOVA has violated Title 18, United States Code, Section 371.

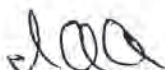
  
\_\_\_\_\_  
David Holt  
Special Agent  
Federal Bureau of Investigation

Reviewed by:

Jay V. Prabhu  
Chief, Cybercrime Unit  
Assistant U.S. Attorney

Alex Ifimie  
Special Assistant U.S. Attorney

Sworn to before me this 28 th day  
of September, 2018

 /s/ \_\_\_\_\_  
Ivan D. Davis  
United States Magistrate Judge

UNITED STATES OF AMERICA

CRIMINAL NO.

(18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq.)

Defendants.

\* \* \* \* \*

The Grand Jury for the District of Columbia charges:

**(Conspiracy to Commit an Offense Against the United States)**

1. In or around 2016, the Russian Federation (“Russia”) operated a military intelligence agency called the Main Intelligence Directorate of the General Staff (“GRU”). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted large-scale cyber operations to interfere with the 2016 U.S. presidential election.

2. Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSANDR VLADIMIROVICH OSADCHUK, and ALEKSEY ALEKSANDROVICH POTEMKIN were GRU officers who knowingly and intentionally conspired with each other, and with persons known and unknown to the Grand Jury (collectively the “Conspirators”), to gain unauthorized access (to “hack”) into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election.

3. Starting in at least March 2016, the Conspirators used a variety of means to hack the email accounts of volunteers and employees of the U.S. presidential campaign of Hillary Clinton (the “Clinton Campaign”), including the email account of the Clinton Campaign’s chairman.

4. By in or around April 2016, the Conspirators also hacked into the computer networks of the Democratic Congressional Campaign Committee (“DCCC”) and the Democratic National Committee (“DNC”). The Conspirators covertly monitored the computers of dozens of DCCC and DNC employees, implanted hundreds of files containing malicious computer code (“malware”), and stole emails and other documents from the DCCC and DNC.

5. By in or around April 2016, the Conspirators began to plan the release of materials stolen from the Clinton Campaign, DCCC, and DNC.

6. Beginning in or around June 2016, the Conspirators staged and released tens of thousands of the stolen emails and documents. They did so using fictitious online personas, including

“DCLeaks” and “Guccifer 2.0.”

7. The Conspirators also used the Guccifer 2.0 persona to release additional stolen documents through a website maintained by an organization (“Organization 1”), that had previously posted documents stolen from U.S. persons, entities, and the U.S. government. The Conspirators continued their U.S. election-interference operations through in or around November 2016.

8. To hide their connections to Russia and the Russian government, the Conspirators used false identities and made false statements about their identities. To further avoid detection, the Conspirators used a network of computers located across the world, including in the United States, and paid for this infrastructure using cryptocurrency.

### **Defendants**

9. Defendant VIKTOR BORISOVICH NETYKSHO (НЕТЫКШО Виктор Борисович) was the Russian military officer in command of Unit 26165, located at 20 Komsomolskiy Prospekt, Moscow, Russia. Unit 26165 had primary responsibility for hacking the DCCC and DNC, as well as the email accounts of individuals affiliated with the Clinton Campaign.

10. Defendant BORIS ALEKSEYEVICH ANTONOV (Антонов Борис Алексеевич) was a Major in the Russian military assigned to Unit 26165. ANTONOV oversaw a department within Unit 26165 dedicated to targeting military, political, governmental, and non-governmental organizations with spearphishing emails and other computer intrusion activity. ANTONOV held the title “Head of Department.” In or around 2016, ANTONOV supervised other co-conspirators who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign.

11. Defendant DMITRIY SERGEYEVICH BADIN (Бадин Дмитрий Сергеевич) was a Russian military officer assigned to Unit 26165 who held the title “Assistant Head of Department.” In or around 2016, BADIN, along with ANTONOV, supervised other co-conspirators who targeted the DCCC, DNC, and individuals affiliated with the Clinton Campaign.

12. Defendant IVAN SERGEYEVICH YERMAKOV (Ермаков Иван Сергеевич) was a Russian military officer assigned to ANTONOV's department within Unit 26165. Since in or around 2010, YERMAKOV used various online personas, including "Kate S. Milton," "James McMorgans," and "Karen W. Millen," to conduct hacking operations on behalf of Unit 26165. In or around March 2016, YERMAKOV participated in hacking at least two email accounts from which campaign-related documents were released through DCLeaks. In or around May 2016, YERMAKOV also participated in hacking the DNC email server and stealing DNC emails that were later released through Organization 1.

13. Defendant ALEKSEY VIKTOROVICH LUKASHEV (Лукашев Алексей Викторович) was a Senior Lieutenant in the Russian military assigned to ANTONOV's department within Unit 26165. LUKASHEV used various online personas, including "Den Katenberg" and "Yuliana Martynova." In or around 2016, LUKASHEV sent spearphishing emails to members of the Clinton Campaign and affiliated individuals, including the chairman of the Clinton Campaign.

14. Defendant SERGEY ALEKSANDROVICH MORGACHEV (Моргачев Сергей Александрович) was a Lieutenant Colonel in the Russian military assigned to Unit 26165. MORGACHEV oversaw a department within Unit 26165 dedicated to developing and managing malware, including a hacking tool used by the GRU known as "X-Agent." During the hacking of the DCCC and DNC networks, MORGACHEV supervised the co-conspirators who developed and monitored the X-Agent malware implanted on those computers.

15. Defendant NIKOLAY YURYEVICH KOZACHEK (Козачек Николай Юрьевич) was a Lieutenant Captain in the Russian military assigned to MORGACHEV's department within Unit 26165. KOZACHEK used a variety of monikers, including "kazak" and "blablabla1234565." KOZACHEK developed, customized, and monitored X-Agent malware used to hack the DCCC

and DNC networks beginning in or around April 2016.

16. Defendant PAVEL VYACHESLAVOVICH YERSHOV (Ершов Павел Вячеславович) was a Russian military officer assigned to MORGACHEV's department within Unit 26165. In or around 2016, YERSHOV assisted KOZACHEK and other co-conspirators in testing and customizing X-Agent malware before actual deployment and use.

17. Defendant ARTEM ANDREYEVICH MALYSHEV (Малышев Артём Андреевич) was a Second Lieutenant in the Russian military assigned to MORGACHEV's department within Unit 26165. MALYSHEV used a variety of monikers, including "djangomagicdev" and "realblatr." In or around 2016, MALYSHEV monitored X-Agent malware implanted on the DCCC and DNC networks.

18. Defendant ALEKSANDR VLADIMIROVICH OSADCHUK (Осадчук Александр Владимирович) was a Colonel in the Russian military and the commanding officer of Unit 74455. Unit 74455 was located at 22 Kirova Street, Khimki, Moscow, a building referred to within the GRU as the "Tower." Unit 74455 assisted in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas, the promotion of those releases, and the publication of anti-Clinton content on social media accounts operated by the GRU.

19. Defendant ALEKSEY ALEKSANDROVICH POTEKIN (Потемкин Алексей Александрович) was an officer in the Russian military assigned to Unit 74455. POTEKIN was a supervisor in a department within Unit 74455 responsible for the administration of computer infrastructure used in cyber operations. Infrastructure and social media accounts administered by POTEKIN's department were used, among other things, to assist in the release of stolen documents through the DCLeaks and Guccifer 2.0 personas.

### **Object of the Conspiracy**

20. The object of the conspiracy was to hack into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 U.S. presidential election.

### **Manner and Means of the Conspiracy**

#### **Spearphishing Operations**

21. ANTONOV, BADIN, YERMAKOV, LUKASHEV, and their co-conspirators targeted victims using a technique known as spearphishing to steal victims' passwords or otherwise gain access to their computers. Beginning by at least March 2016, the Conspirators targeted over 300 individuals affiliated with the Clinton Campaign, DCCC, and DNC.

- a. For example, on or about March 19, 2016, LUKASHEV and his co-conspirators created and sent a spearphishing email to the chairman of the Clinton Campaign. LUKASHEV used the account "john356gh" at an online service that abbreviated lengthy website addresses (referred to as a "URL-shortening service"). LUKASHEV used the account to mask a link contained in the spearphishing email, which directed the recipient to a GRU-created website. LUKASHEV altered the appearance of the sender email address in order to make it look like the email was a security notification from Google (a technique known as "spoofing"), instructing the user to change his password by clicking the embedded link. Those instructions were followed. On or about March 21, 2016, LUKASHEV, YERMAKOV, and their co-conspirators stole the contents of the chairman's email account, which consisted of over 50,000 emails.
- b. Starting on or about March 19, 2016, LUKASHEV and his co-conspirators sent spearphishing emails to the personal accounts of other individuals affiliated with

the Clinton Campaign, including its campaign manager and a senior foreign policy advisor. On or about March 25, 2016, LUKASHEV used the same john356gh account to mask additional links included in spearphishing emails sent to numerous individuals affiliated with the Clinton Campaign, including Victims 1 and 2. LUKASHEV sent these emails from the Russia-based email account hi.mymail@yandex.com that he spoofed to appear to be from Google.

- c. On or about March 28, 2016, YERMAKOV researched the names of Victims 1 and 2 and their association with Clinton on various social media sites. Through their spearphishing operations, LUKASHEV, YERMAKOV, and their co-conspirators successfully stole email credentials and thousands of emails from numerous individuals affiliated with the Clinton Campaign. Many of these stolen emails, including those from Victims 1 and 2, were later released by the Conspirators through DCLeaks.
- d. On or about April 6, 2016, the Conspirators created an email account in the name (with a one-letter deviation from the actual spelling) of a known member of the Clinton Campaign. The Conspirators then used that account to send spearphishing emails to the work accounts of more than thirty different Clinton Campaign employees. In the spearphishing emails, LUKASHEV and his co-conspirators embedded a link purporting to direct the recipient to a document titled “hillary-clinton-favorable-rating.xlsx.” In fact, this link directed the recipients’ computers to a GRU-created website.

22. The Conspirators spearphished individuals affiliated with the Clinton Campaign throughout the summer of 2016. For example, on or about July 27, 2016, the Conspirators

attempted after hours to spearfish for the first time email accounts at a domain hosted by a third-party provider and used by Clinton's personal office. At or around the same time, they also targeted seventy-six email addresses at the domain for the Clinton Campaign.

#### Hacking into the DCCC Network

23. Beginning in or around March 2016, the Conspirators, in addition to their spearphishing efforts, researched the DCCC and DNC computer networks to identify technical specifications and vulnerabilities.

- a. For example, beginning on or about March 15, 2016, YERMAKOV ran a technical query for the DNC's internet protocol configurations to identify connected devices.
- b. On or about the same day, YERMAKOV searched for open-source information about the DNC network, the Democratic Party, and Hillary Clinton.
- c. On or about April 7, 2016, YERMAKOV ran a technical query for the DCCC's internet protocol configurations to identify connected devices.

24. By in or around April 2016, within days of YERMAKOV's searches regarding the DCCC, the Conspirators hacked into the DCCC computer network. Once they gained access, they installed and managed different types of malware to explore the DCCC network and steal data.

- a. On or about April 12, 2016, the Conspirators used the stolen credentials of a DCCC Employee ("DCCC Employee 1") to access the DCCC network. DCCC Employee 1 had received a spearphishing email from the Conspirators on or about April 6, 2016, and entered her password after clicking on the link.
- b. Between in or around April 2016 and June 2016, the Conspirators installed multiple versions of their X-Agent malware on at least ten DCCC computers, which allowed them to monitor individual employees' computer activity, steal passwords, and maintain access to the DCCC network.

- c. X-Agent malware implanted on the DCCC network transmitted information from the victims' computers to a GRU-leased server located in Arizona. The Conspirators referred to this server as their "AMS" panel. KOZACHEK, MALYSHEV, and their co-conspirators logged into the AMS panel to use X-Agent's keylog and screenshot functions in the course of monitoring and surveilling activity on the DCCC computers. The keylog function allowed the Conspirators to capture keystrokes entered by DCCC employees. The screenshot function allowed the Conspirators to take pictures of the DCCC employees' computer screens.
- d. For example, on or about April 14, 2016, the Conspirators repeatedly activated X-Agent's keylog and screenshot functions to surveil DCCC Employee 1's computer activity over the course of eight hours. During that time, the Conspirators captured DCCC Employee 1's communications with co-workers and the passwords she entered while working on fundraising and voter outreach projects. Similarly, on or about April 22, 2016, the Conspirators activated X-Agent's keylog and screenshot functions to capture the discussions of another DCCC Employee ("DCCC Employee 2") about the DCCC's finances, as well as her individual banking information and other personal topics.

25. On or about April 19, 2016, KOZACHEK, YERSHOV, and their co-conspirators remotely configured an overseas computer to relay communications between X-Agent malware and the AMS panel and then tested X-Agent's ability to connect to this computer. The Conspirators referred to this computer as a "middle server." The middle server acted as a proxy to obscure the connection between malware at the DCCC and the Conspirators' AMS panel. On or about April

20, 2016, the Conspirators directed X-Agent malware on the DCCC computers to connect to this middle server and receive directions from the Conspirators.

#### Hacking into the DNC Network

26. On or about April 18, 2016, the Conspirators hacked into the DNC's computers through their access to the DCCC network. The Conspirators then installed and managed different types of malware (as they did in the DCCC network) to explore the DNC network and steal documents.

- a. On or about April 18, 2016, the Conspirators activated X-Agent's keylog and screenshot functions to steal credentials of a DCCC employee who was authorized to access the DNC network. The Conspirators hacked into the DNC network from the DCCC network using stolen credentials. By in or around June 2016, they gained access to approximately thirty-three DNC computers.
- b. In or around April 2016, the Conspirators installed X-Agent malware on the DNC network, including the same versions installed on the DCCC network. MALYSHEV and his co-conspirators monitored the X-Agent malware from the AMS panel and captured data from the victim computers. The AMS panel collected thousands of keylog and screenshot results from the DCCC and DNC computers, such as a screenshot and keystroke capture of DCCC Employee 2 viewing the DCCC's online banking information.

#### Theft of DCCC and DNC Documents

27. The Conspirators searched for and identified computers within the DCCC and DNC networks that stored information related to the 2016 U.S. presidential election. For example, on or about April 15, 2016, the Conspirators searched one hacked DCCC computer for terms that included "hillary," "cruz," and "trump." The Conspirators also copied select DCCC folders, including "Benghazi Investigations." The Conspirators targeted computers containing information

such as opposition research and field operation plans for the 2016 elections.

28. To enable them to steal a large number of documents at once without detection, the Conspirators used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks. The Conspirators then used other GRU malware, known as “X-Tunnel,” to move the stolen documents outside the DCCC and DNC networks through encrypted channels.

- a. For example, on or about April 22, 2016, the Conspirators compressed gigabytes of data from DNC computers, including opposition research. The Conspirators later moved the compressed DNC data using X-Tunnel to a GRU-leased computer located in Illinois.
- b. On or about April 28, 2016, the Conspirators connected to and tested the same computer located in Illinois. Later that day, the Conspirators used X-Tunnel to connect to that computer to steal additional documents from the DCCC network.

29. Between on or about May 25, 2016 and June 1, 2016, the Conspirators hacked the DNC Microsoft Exchange Server and stole thousands of emails from the work accounts of DNC employees. During that time, YERMAKOV researched PowerShell commands related to accessing and managing the Microsoft Exchange Server.

30. On or about May 30, 2016, MALYSHEV accessed the AMS panel in order to upgrade custom AMS software on the server. That day, the AMS panel received updates from approximately thirteen different X-Agent malware implants on DCCC and DNC computers.

31. During the hacking of the DCCC and DNC networks, the Conspirators covered their tracks by intentionally deleting logs and computer files. For example, on or about May 13, 2016, the Conspirators cleared the event logs from a DNC computer. On or about June 20, 2016, the

Conspirators deleted logs from the AMS panel that documented their activities on the panel, including the login history.

Efforts to Remain on the DCCC and DNC Networks

32. Despite the Conspirators' efforts to hide their activity, beginning in or around May 2016, both the DCCC and DNC became aware that they had been hacked and hired a security company ("Company 1") to identify the extent of the intrusions. By in or around June 2016, Company 1 took steps to exclude intruders from the networks. Despite these efforts, a Linux-based version of X-Agent, programmed to communicate with the GRU-registered domain linuxknl.net, remained on the DNC network until in or around October 2016.

33. In response to Company 1's efforts, the Conspirators took countermeasures to maintain access to the DCCC and DNC networks.

- a. On or about May 31, 2016, YERMAKOV searched for open-source information about Company 1 and its reporting on X-Agent and X-Tunnel. On or about June 1, 2016, the Conspirators attempted to delete traces of their presence on the DCCC network using the computer program CCleaner.
- b. On or about June 14, 2016, the Conspirators registered the domain actblues.com, which mimicked the domain of a political fundraising platform that included a DCCC donations page. Shortly thereafter, the Conspirators used stolen DCCC credentials to modify the DCCC website and redirect visitors to the actblues.com domain.
- c. On or about June 20, 2016, after Company 1 had disabled X-Agent on the DCCC network, the Conspirators spent over seven hours unsuccessfully trying to connect to X-Agent. The Conspirators also tried to access the DCCC network using previously stolen credentials.

34. In or around September 2016, the Conspirators also successfully gained access to DNC computers hosted on a third-party cloud-computing service. These computers contained test applications related to the DNC's analytics. After conducting reconnaissance, the Conspirators gathered data by creating backups, or "snapshots," of the DNC's cloud-based systems using the cloud provider's own technology. The Conspirators then moved the snapshots to cloud-based accounts they had registered with the same service, thereby stealing the data from the DNC.

#### Stolen Documents Released through DCLeaks

35. More than a month before the release of any documents, the Conspirators constructed the online persona DCLeaks to release and publicize stolen election-related documents. On or about April 19, 2016, after attempting to register the domain electionleaks.com, the Conspirators registered the domain dcleaks.com through a service that anonymized the registrant. The funds used to pay for the dcleaks.com domain originated from an account at an online cryptocurrency service that the Conspirators also used to fund the lease of a virtual private server registered with the operational email account dirbinsaabol@mail.com. The dirbinsaabol email account was also used to register the john356gh URL-shortening account used by LUKASHEV to spearphish the Clinton Campaign chairman and other campaign-related individuals.

36. On or about June 8, 2016, the Conspirators launched the public website dcleaks.com, which they used to release stolen emails. Before it shut down in or around March 2017, the site received over one million page views. The Conspirators falsely claimed on the site that DCLeaks was started by a group of "American hacktivists," when in fact it was started by the Conspirators.

37. Starting in or around June 2016 and continuing through the 2016 U.S. presidential election, the Conspirators used DCLeaks to release emails stolen from individuals affiliated with the Clinton Campaign. The Conspirators also released documents they had stolen in other spearphishing operations, including those they had conducted in 2015 that collected emails from individuals

affiliated with the Republican Party.

38. On or about June 8, 2016, and at approximately the same time that the dcleaks.com website was launched, the Conspirators created a DCLeaks Facebook page using a preexisting social media account under the fictitious name “Alice Donovan.” In addition to the DCLeaks Facebook page, the Conspirators used other social media accounts in the names of fictitious U.S. persons such as “Jason Scott” and “Richard Gingrey” to promote the DCLeaks website. The Conspirators accessed these accounts from computers managed by POTEMKIN and his co-conspirators.

39. On or about June 8, 2016, the Conspirators created the Twitter account @dcleaks\_. The Conspirators operated the @dcleaks\_ Twitter account from the same computer used for other efforts to interfere with the 2016 U.S. presidential election. For example, the Conspirators used the same computer to operate the Twitter account @BaltimoreIsWhr, through which they encouraged U.S. audiences to “[j]oin our flash mob” opposing Clinton and to post images with the hashtag #BlacksAgainstHillary.

#### Stolen Documents Released through Guccifer 2.0

40. On or about June 14, 2016, the DNC—through Company 1—publicly announced that it had been hacked by Russian government actors. In response, the Conspirators created the online persona Guccifer 2.0 and falsely claimed to be a lone Romanian hacker to undermine the allegations of Russian responsibility for the intrusion.

41. On or about June 15, 2016, the Conspirators logged into a Moscow-based server used and managed by Unit 74455 and, between 4:19 PM and 4:56 PM Moscow Standard Time, searched for certain words and phrases, including:

Search Term(s)
<b>“some hundred sheets”</b>
<b>“some hundreds of sheets”</b>
<b>dcleaks</b>
<b>illuminati</b>
<b>широко известный перевод</b> [widely known translation]
<b>“worldwide known”</b>
<b>“think twice about”</b>
<b>“company’s competence”</b>

42. Later that day, at 7:02 PM Moscow Standard Time, the online persona Guccifer 2.0 published its first post on a blog site created through WordPress. Titled “DNC’s servers hacked by a lone hacker,” the post used numerous English words and phrases that the Conspirators had searched for earlier that day (bolded below):

**Worldwide known** cyber security company [Company 1] announced that the Democratic National Committee (DNC) servers had been hacked by “sophisticated” hacker groups.

I’m very pleased the company appreciated my skills so highly))) [. . .]

Here are just a few docs from many thousands I extracted when hacking into DNC’s network. [. . .]

**Some hundred sheets!** This’s a serious case, isn’t it? [. . .]

I guess [Company 1] customers should **think twice about company’s competence.**

F[\*\*\*] the **Illuminati** and their conspiracies!!!!!!!!!! F[\*\*\*]  
[Company 1]!!!!!!!!!!

43. Between in or around June 2016 and October 2016, the Conspirators used Guccifer 2.0 to release documents through WordPress that they had stolen from the DCCC and DNC. The Conspirators, posing as Guccifer 2.0, also shared stolen documents with certain individuals.

a. On or about August 15, 2016, the Conspirators, posing as Guccifer 2.0, received a

request for stolen documents from a candidate for the U.S. Congress. The Conspirators responded using the Guccifer 2.0 persona and sent the candidate stolen documents related to the candidate's opponent.

- b. On or about August 22, 2016, the Conspirators, posing as Guccifer 2.0, transferred approximately 2.5 gigabytes of data stolen from the DCCC to a then-registered state lobbyist and online source of political news. The stolen data included donor records and personal identifying information for more than 2,000 Democratic donors.
- c. On or about August 22, 2016, the Conspirators, posing as Guccifer 2.0, sent a reporter stolen documents pertaining to the Black Lives Matter movement. The reporter responded by discussing when to release the documents and offering to write an article about their release.

44. The Conspirators, posing as Guccifer 2.0, also communicated with U.S. persons about the release of stolen documents. On or about August 15, 2016, the Conspirators, posing as Guccifer 2.0, wrote to a person who was in regular contact with senior members of the presidential campaign of Donald J. Trump, "thank u for writing back . . . do u find anyt[h]ing interesting in the docs i posted?" On or about August 17, 2016, the Conspirators added, "please tell me if i can help u anyhow . . . it would be a great pleasure to me." On or about September 9, 2016, the Conspirators, again posing as Guccifer 2.0, referred to a stolen DCCC document posted online and asked the person, "what do u think of the info on the turnout model for the democrats entire presidential campaign." The person responded, "[p]retty standard."

45. The Conspirators conducted operations as Guccifer 2.0 and DCLeaks using overlapping computer infrastructure and financing.

- a. For example, between on or about March 14, 2016 and April 28, 2016, the

Conspirators used the same pool of bitcoin funds to purchase a virtual private network (“VPN”) account and to lease a server in Malaysia. In or around June 2016, the Conspirators used the Malaysian server to host the dcleaks.com website. On or about July 6, 2016, the Conspirators used the VPN to log into the @Guccifer\_2 Twitter account. The Conspirators opened that VPN account from the same server that was also used to register malicious domains for the hacking of the DCCC and DNC networks.

- b. On or about June 27, 2016, the Conspirators, posing as Guccifer 2.0, contacted a U.S. reporter with an offer to provide stolen emails from “Hillary Clinton’s staff.” The Conspirators then sent the reporter the password to access a nonpublic, password-protected portion of dcleaks.com containing emails stolen from Victim 1 by LUKASHEV, YERMAKOV, and their co-conspirators in or around March 2016.

46. On or about January 12, 2017, the Conspirators published a statement on the Guccifer 2.0 WordPress blog, falsely claiming that the intrusions and release of stolen documents had “totally no relation to the Russian government.”

#### Use of Organization 1

47. In order to expand their interference in the 2016 U.S. presidential election, the Conspirators transferred many of the documents they stole from the DNC and the chairman of the Clinton Campaign to Organization 1. The Conspirators, posing as Guccifer 2.0, discussed the release of the stolen documents and the timing of those releases with Organization 1 to heighten their impact on the 2016 U.S. presidential election.

- a. On or about June 22, 2016, Organization 1 sent a private message to Guccifer 2.0 to “[s]end any new material [stolen from the DNC] here for us to review and it will

have a much higher impact than what you are doing.” On or about July 6, 2016, Organization 1 added, “if you have anything hillary related we want it in the next tweeo [*sic*] days prefable [*sic*] because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after.” The Conspirators responded, “ok . . . i see.” Organization 1 explained, “we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting.”

- b. After failed attempts to transfer the stolen documents starting in late June 2016, on or about July 14, 2016, the Conspirators, posing as Guccifer 2.0, sent Organization 1 an email with an attachment titled “wk dnc link1.txt.gpg.” The Conspirators explained to Organization 1 that the encrypted file contained instructions on how to access an online archive of stolen DNC documents. On or about July 18, 2016, Organization 1 confirmed it had “the 1Gb or so archive” and would make a release of the stolen documents “this week.”

48. On or about July 22, 2016, Organization 1 released over 20,000 emails and other documents stolen from the DNC network by the Conspirators. This release occurred approximately three days before the start of the Democratic National Convention. Organization 1 did not disclose Guccifer 2.0’s role in providing them. The latest-in-time email released through Organization 1 was dated on or about May 25, 2016, approximately the same day the Conspirators hacked the DNC Microsoft Exchange Server.

49. On or about October 7, 2016, Organization 1 released the first set of emails from the chairman of the Clinton Campaign that had been stolen by LUKASHEV and his co-conspirators. Between on or about October 7, 2016 and November 7, 2016, Organization 1 released

approximately thirty-three tranches of documents that had been stolen from the chairman of the Clinton Campaign. In total, over 50,000 stolen documents were released.

### **Statutory Allegations**

50. Paragraphs 1 through 49 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

51. From at least in or around March 2016 through November 2016, in the District of Columbia and elsewhere, Defendants NETYKSHO, ANTONOV, BADIN, YERMAKOV, LUKASHEV, MORGACHEV, KOZACHEK, YERSHOV, MALYSHEV, OSADCHUK, and POTEMKIN, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit offenses against the United States, namely:

- a. To knowingly access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, where the value of the information obtained exceeded \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B); and
- b. To knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, and where the offense did cause and, if completed, would have caused, loss aggregating \$5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

52. In furtherance of the Conspiracy and to effect its illegal objects, the Conspirators committed the overt acts set forth in paragraphs 1 through 19, 21 through 49, 55, and 57 through

64, which are re-alleged and incorporated by reference as if fully set forth herein.

53. In furtherance of the Conspiracy, and as set forth in paragraphs 1 through 19, 21 through 49, 55, and 57 through 64, the Conspirators knowingly falsely registered a domain name and knowingly used that domain name in the course of committing an offense, namely, the Conspirators registered domains, including dcleaks.com and actblues.com, with false names and addresses, and used those domains in the course of committing the felony offense charged in Count One.

All in violation of Title 18, United States Code, Sections 371 and 3559(g)(1).

**COUNTS TWO THROUGH NINE**  
**(Aggravated Identity Theft)**

54. Paragraphs 1 through 19, 21 through 49, and 57 through 64 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

55. On or about the dates specified below, in the District of Columbia and elsewhere, Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSANDR VLADIMIROVICH OSADCHUK, and ALEKSEY ALEKSANDROVICH POTEKIN did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), namely, computer fraud in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B), knowing that the means of identification belonged to another real person:

Count	Approximate Date	Victim	Means of Identification
2	March 21, 2016	Victim 3	Username and password for personal email account
3	March 25, 2016	Victim 1	Username and password for personal email account
4	April 12, 2016	Victim 4	Username and password for DCCC computer network
5	April 15, 2016	Victim 5	Username and password for DCCC computer network
6	April 18, 2016	Victim 6	Username and password for DCCC computer network
7	May 10, 2016	Victim 7	Username and password for DNC computer network
8	June 2, 2016	Victim 2	Username and password for personal email account
9	July 6, 2016	Victim 8	Username and password for personal email account

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

**COUNT TEN**  
**(Conspiracy to Launder Money)**

56. Paragraphs 1 through 19, 21 through 49, and 55 are re-alleged and incorporated by reference as if fully set forth herein.

57. To facilitate the purchase of infrastructure used in their hacking activity—including hacking into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election and releasing the stolen documents—the Defendants conspired to launder the equivalent of more than \$95,000 through a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin.

58. Although the Conspirators caused transactions to be conducted in a variety of currencies, including U.S. dollars, they principally used bitcoin when purchasing servers, registering domains, and otherwise making payments in furtherance of hacking activity. Many of these payments were

processed by companies located in the United States that provided payment processing services to hosting companies, domain registrars, and other vendors both international and domestic. The use of bitcoin allowed the Conspirators to avoid direct relationships with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds.

59. All bitcoin transactions are added to a public ledger called the Blockchain, but the Blockchain identifies the parties to each transaction only by alpha-numeric identifiers known as bitcoin addresses. To further avoid creating a centralized paper trail of all of their purchases, the Conspirators purchased infrastructure using hundreds of different email accounts, in some cases using a new account for each purchase. The Conspirators used fictitious names and addresses in order to obscure their identities and their links to Russia and the Russian government. For example, the dcleaks.com domain was registered and paid for using the fictitious name “Carrie Feehan” and an address in New York. In some cases, as part of the payment process, the Conspirators provided vendors with nonsensical addresses such as “usa Denver AZ,” “ghfgh ghfhgh fdgfdg WA,” and “1 2 dwd District of Columbia.”

60. The Conspirators used several dedicated email accounts to track basic bitcoin transaction information and to facilitate bitcoin payments to vendors. One of these dedicated accounts, registered with the username “gfadel47,” received hundreds of bitcoin payment requests from approximately 100 different email accounts. For example, on or about February 1, 2016, the gfadel47 account received the instruction to “[p]lease send *exactly* **0.026043** bitcoin to” a certain thirty-four character bitcoin address. Shortly thereafter, a transaction matching those exact instructions was added to the Blockchain.

61. On occasion, the Conspirators facilitated bitcoin payments using the same computers that they used to conduct their hacking activity, including to create and send test spearphishing emails.

Additionally, one of these dedicated accounts was used by the Conspirators in or around 2015 to renew the registration of a domain (linuxkrnl.net) encoded in certain X-Agent malware installed on the DNC network.

62. The Conspirators funded the purchase of computer infrastructure for their hacking activity in part by “mining” bitcoin. Individuals and entities can mine bitcoin by allowing their computing power to be used to verify and record payments on the bitcoin public ledger, a service for which they are rewarded with freshly-minted bitcoin. The pool of bitcoin generated from the GRU’s mining activity was used, for example, to pay a Romanian company to register the domain dcleaks.com through a payment processing company located in the United States.

63. In addition to mining bitcoin, the Conspirators acquired bitcoin through a variety of means designed to obscure the origin of the funds. This included purchasing bitcoin through peer-to-peer exchanges, moving funds through other digital currencies, and using pre-paid cards. They also enlisted the assistance of one or more third-party exchangers who facilitated layered transactions through digital currency exchange platforms providing heightened anonymity.

64. The Conspirators used the same funding structure—and in some cases, the very same pool of funds—to purchase key accounts, servers, and domains used in their election-related hacking activity.

- a. The bitcoin mining operation that funded the registration payment for dcleaks.com also sent newly-minted bitcoin to a bitcoin address controlled by “Daniel Farrell,” the persona that was used to renew the domain linuxkrnl.net. The bitcoin mining operation also funded, through the same bitcoin address, the purchase of servers and domains used in the GRU’s spearphishing operations, including accounts-qooqle.com and account-goooogle.com.

- b. On or about March 14, 2016, using funds in a bitcoin address, the Conspirators purchased a VPN account, which they later used to log into the @Guccifer\_2 Twitter account. The remaining funds from that bitcoin address were then used on or about April 28, 2016, to lease a Malaysian server that hosted the dcleaks.com website.
- c. The Conspirators used a different set of fictitious names (including “Ward DeClaus” and “Mike Long”) to send bitcoin to a U.S. company in order to lease a server used to administer X-Tunnel malware implanted on the DCCC and DNC networks, and to lease two servers used to hack the DNC’s cloud network.

### **Statutory Allegations**

65. From at least in or around 2015 through 2016, within the District of Columbia and elsewhere, Defendants VIKTOR BORISOVICH NETYKSHO, BORIS ALEKSEYEVICH ANTONOV, DMITRIY SERGEYEVICH BADIN, IVAN SERGEYEVICH YERMAKOV, ALEKSEY VIKTOROVICH LUKASHEV, SERGEY ALEKSANDROVICH MORGACHEV, NIKOLAY YURYEVICH KOZACHEK, PAVEL VYACHESLAVOVICH YERSHOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSANDR VLADIMIROVICH OSADCHUK, and ALEKSEY ALEKSANDROVICH POTEMKIN, together with others, known and unknown to the Grand Jury, did knowingly and intentionally conspire to transport, transmit, and transfer monetary instruments and funds to a place in the United States from and through a place outside the United States and from a place in the United States to and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, namely, a violation of Title 18, United States Code, Section 1030, contrary to Title 18, United States Code, Section 1956(a)(2)(A).

All in violation of Title 18, United States Code, Section 1956(h).

**COUNT ELEVEN**

**(Conspiracy to Commit an Offense Against the United States)**

66. Paragraphs 1 through 8 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

**Defendants**

67. Paragraph 18 of this Indictment relating to ALEKSANDR VLADIMIROVICH OSADCHUK is re-alleged and incorporated by reference as if fully set forth herein.

68. Defendant ANATOLIY SERGEYEVICH KOVALEV (Ковалев Анатолий Сергеевич) was an officer in the Russian military assigned to Unit 74455 who worked in the GRU's 22 Kirova Street building (the Tower).

69. Defendants OSADCHUK and KOVALEV were GRU officers who knowingly and intentionally conspired with each other and with persons, known and unknown to the Grand Jury, to hack into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections.

**Object of the Conspiracy**

70. The object of the conspiracy was to hack into protected computers of persons and entities charged with the administration of the 2016 U.S. elections in order to access those computers and steal voter data and other information stored on those computers.

**Manner and Means of the Conspiracy**

71. In or around June 2016, KOVALEV and his co-conspirators researched domains used by U.S. state boards of elections, secretaries of state, and other election-related entities for website vulnerabilities. KOVALEV and his co-conspirators also searched for state political party email addresses, including filtered queries for email addresses listed on state Republican Party websites.

72. In or around July 2016, KOVALEV and his co-conspirators hacked the website of a state board of elections (“SBOE 1”) and stole information related to approximately 500,000 voters, including names, addresses, partial social security numbers, dates of birth, and driver’s license numbers.

73. In or around August 2016, KOVALEV and his co-conspirators hacked into the computers of a U.S. vendor (“Vendor 1”) that supplied software used to verify voter registration information for the 2016 U.S. elections. KOVALEV and his co-conspirators used some of the same infrastructure to hack into Vendor 1 that they had used to hack into SBOE 1.

74. In or around August 2016, the Federal Bureau of Investigation issued an alert about the hacking of SBOE 1 and identified some of the infrastructure that was used to conduct the hacking. In response, KOVALEV deleted his search history. KOVALEV and his co-conspirators also deleted records from accounts used in their operations targeting state boards of elections and similar election-related entities.

75. In or around October 2016, KOVALEV and his co-conspirators further targeted state and county offices responsible for administering the 2016 U.S. elections. For example, on or about October 28, 2016, KOVALEV and his co-conspirators visited the websites of certain counties in Georgia, Iowa, and Florida to identify vulnerabilities.

76. In or around November 2016 and prior to the 2016 U.S. presidential election, KOVALEV and his co-conspirators used an email account designed to look like a Vendor 1 email address to send over 100 spearphishing emails to organizations and personnel involved in administering elections in numerous Florida counties. The spearphishing emails contained malware that the Conspirators embedded into Word documents bearing Vendor 1’s logo.

#### **Statutory Allegations**

77. Between in or around June 2016 and November 2016, in the District of Columbia and

elsewhere, Defendants OSADCHUK and KOVALEV, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit offenses against the United States, namely:

- a. To knowingly access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, where the value of the information obtained exceeded \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B); and
- b. To knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, and where the offense did cause and, if completed, would have caused, loss aggregating \$5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, and damage affecting at least ten protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

78. In furtherance of the Conspiracy and to effect its illegal objects, OSADCHUK, KOVALEV, and their co-conspirators committed the overt acts set forth in paragraphs 67 through 69 and 71 through 76, which are re-alleged and incorporated by reference as if fully set forth herein.

All in violation of Title 18, United States Code, Section 371.

#### **FORFEITURE ALLEGATION**

79. Pursuant to Federal Rule of Criminal Procedure 32.2, notice is hereby given to Defendants that the United States will seek forfeiture as part of any sentence in the event of Defendants' convictions under Counts One, Ten, and Eleven of this Indictment. Pursuant to Title 18, United

States Code, Sections 982(a)(2) and 1030(i), upon conviction of the offenses charged in Counts One and Eleven, Defendants NETYKSHO, ANTONOV, BADIN, YERMAKOV, LUKASHEV, MORGACHEV, KOZACHEK, YERSHOV, MALYSHEV, OSADCHUK, POTEMKIN, and KOVALEV shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds obtained directly or indirectly as a result of such violation, and any personal property that was used or intended to be used to commit or to facilitate the commission of such offense. Pursuant to Title 18, United States Code, Section 982(a)(1), upon conviction of the offense charged in Count Ten, Defendants NETYKSHO, ANTONOV, BADIN, YERMAKOV, LUKASHEV, MORGACHEV, KOZACHEK, YERSHOV, MALYSHEV, OSADCHUK, and POTEMKIN shall forfeit to the United States any property, real or personal, involved in such offense, and any property traceable to such property. Notice is further given that, upon conviction, the United States intends to seek a judgment against each Defendant for a sum of money representing the property described in this paragraph, as applicable to each Defendant (to be offset by the forfeiture of any specific property).

#### **Substitute Assets**


80. If any of the property described above as being subject to forfeiture, as a result of any act or omission of any Defendant --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property that cannot be subdivided without difficulty;

it is the intent of the United States of America, pursuant to Title 18, United States Code, Section

982(b) and Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853, to seek forfeiture of any other property of said Defendant.

Pursuant to 18 U.S.C. §§ 982 and 1030(i); 28 U.S.C. § 2461(c).

  
Robert S. Mueller, III  
Special Counsel  
U.S. Department of Justice

A TRUE BILL:

\_\_\_\_\_  
Foreperson

Date: July 13, 2018

**FILED**

**MAY 29 2019**

Clerk, U.S. District and  
Bankruptcy Courts

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA

v.

CONCORD MANAGEMENT &  
CONSULTING LLC,

*Defendant.*

Criminal Action No. 18-cr-32-2 (DLF)

**Filed Under Seal**

As stated during yesterday's sealed motions hearing, it is

**ORDERED** that the parties shall abide by Local Criminal Rule 57.7(b) and that the willful failure to do so in the future will result in the initiation of contempt proceedings;

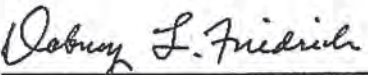
**ORDERED** that the government shall refrain from making or authorizing any public statement that links the alleged conspiracy in the indictment to the Russian government or its agencies;

**ORDERED** that to the extent the government makes or authorizes any public statement about the allegations in the indictment, such statement must make clear that (1) the government is summarizing the allegations in the indictment, which remain unproven, and (2) the government does not express an opinion on the defendants' guilt or innocence or the strength of the evidence in this case.

It is further **ORDERED** that the parties shall file supplemental briefs under seal addressing the following questions:

1. Can and should the Court defer consideration of Concord's motion for an order to show cause until after trial, to ensure a fair and impartial trial?
2. If the Court concludes that the government has violated Local Criminal Rule 57.7(b), does the Court have discretion to decline to initiate contempt proceedings and to instead address the violation through alternative means, such as a Rule 57.7(c) order, targeted voir dire questioning, and/or the Court's inherent disciplinary authority?
3. If the Court enters an order regulating the parties' public statements about this case pursuant to Local Criminal Rule 57.7(c), what terms should that order contain? Specifically, how should the Court address the Mueller Report, which has already been disseminated publicly in its current form and which may or may not be disseminated with certain redactions removed, pending the resolution of negotiations between the Department of Justice and Congress and various other court matters?

Both parties shall file their respective memoranda under seal on or before June 5, 2019 and shall file any response to the other party's memorandum under seal on or before June 12, 2019.

  
DABNEY L. FRIEDRICH  
United States District Judge

May 29, 2019

## Exhibit I



**U.S. Department of Justice**

National Security Division

---

Washington, D.C. 20530

Mr. Ty Clevenger  
212 S. Oxford Street. #7D  
Brooklyn, NY 112217  
Via e-mail to: tyclevenger@yahoo.com

FOI/PA #20-338

16 November 2021

Dear Mr. Clevenger:

This is the National Security Division's (NSD) final response to your Freedom of Information Act (FOIA) request dated June 18, 2020 to the Mail Referral Unit (MRU). The MRU forwarded your request to NSD, and we received your request on June 23, 2020. We have assigned it NSD #20-338.

Specifically, your request states:

1. *I request the opportunity to view all documents, records, communications and/or other tangible evidence reflecting or pertaining to surveillance of Edward Butowsky of Texas or Matt Couch of Arkansas. The term "surveillance" includes, but is not limited to, any attempt to hack into the computers, phones, other electronic devices, and/or online accounts of Mr. Butowsky or Mr. Couch. If any information obtained by surveillance was relayed to third parties, that information should be produced for inspection.*
2. *I request the opportunity to view all documents, records, communications and/or other tangible evidence pertaining to whether former Central Intelligence Agency Director David Petraeus mishandled classified information or sold such information during his tenure as CIA director. This request includes, but is not limited to, documents, records, communications and/or other tangible evidence in the possession of the Office of the Inspector General of the CIA and/or the Office of the Intelligence Community Inspector General. This request further includes, but is not limited to, any draft indictments, draft arrest warrants, actual arrest warrants, and/or records of arrest.*

Regarding item 1 of your request, the NSD, Office of Intelligence represents the government before the Foreign Intelligence Surveillance Court and is responsible for preparing and filing all applications for Court orders pursuant to FISA and maintains files documenting those applications and orders. Because confirming or denying whether records responsive to

FOIA requests exist would disclose information exempt from disclosure under FOIA, we do not search these records in response to FOIA requests. Any such information is properly classified under Executive Order 13526. To confirm or deny the existence of such records in each case would reveal properly classified information regarding intelligence sources and methods. Accordingly, we can neither confirm nor deny the existence of records in these files responsive to your request pursuant to 5 U.S.C. 552(b)(1).

Regarding item 2 of your request, a search of the Counterintelligence and Export Control Section of NSD was conducted. We located records responsive to your request. We are releasing them in full. Copies are attached. We also located a record which originated in the Office of the United States Attorney for the Eastern District of Virginia. We have referred that record to the Executive Office for United States Attorneys for review and direct response to you.

As this matter is already in litigation, we are omitting our standard appeal paragraph. If you have any questions concerning this response please contact Assistant United States Attorney, Andrea Parker of the Eastern District of Texas at (409) 839-2538.

Sincerely,



Kevin G. Tiernan  
Records and FOIA

Enclosures

**FILED**  
CHARLOTTE, NC  
MAR 3 2015  
U.S. DISTRICT COURT  
WESTERN DISTRICT OF NC

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF NORTH CAROLINA  
CHARLOTTE DIVISION

UNITED STATES OF AMERICA )

v. )

DAVID HOWELL PETRAEUS )

DOCKET NO. 3:15 CR 47

**FACTUAL BASIS**

NOW COMES the United States of America, by and through Anne M. Tompkins, United States Attorney for the Western District of North Carolina, James P. Melendres, Trial Attorney, Jill Westmoreland Rose, Assistant United States Attorney, and Richard S. Scott, Trial Attorney, and hereby files this Factual Basis in support of the Plea Agreement filed simultaneously in this matter.

This Factual Basis does not attempt to set forth all of the facts known to the United States at this time. By their signatures below, the parties expressly agree that there is a factual basis for the guilty plea that the defendant will tender pursuant to the Plea Agreement. The parties also agree that this Factual Basis may, but need not, be used by the United States Probation Office and the Court in determining the applicable advisory guideline range under the United States Sentencing Guidelines or the appropriate sentence under 18 U.S.C. § 3553(a). The defendant agrees not to object to any fact set forth below being used by the Court or the United States Probation Office to determine the applicable advisory guideline range or the appropriate sentence under 18 U.S.C. § 3553(a). The parties' agreement does not preclude either party from hereafter presenting the Court with additional facts which do not contradict facts to which the parties have agreed not to object and which are relevant to the Court's guideline computations, to 18 U.S.C. § 3553 factors, or to the Court's overall sentencing decision.

The parties stipulate that the allegations in the Bill of Information and the following facts are true and correct, and that had the matter gone to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence. Specifically, the evidence would establish, at a minimum, the following facts:

At all relevant times,

#### **The Defendant**

1. Defendant DAVID HOWELL PETRAEUS, a citizen of the United States and resident of Arlington, Virginia, was a United States Army four-star general when he retired from the Army on or about August 31, 2011. From on or about July 4, 2010, to on or about July 18, 2011, defendant DAVID HOWELL PETRAEUS served as Commander of the International Security Assistance Force ("ISAF") in Afghanistan. From on or about September 6, 2011, to on or about November 9, 2012, defendant DAVID HOWELL PETRAEUS served as Director of the Central Intelligence Agency ("CIA").

#### **Classified Information**

2. Those persons with security clearances granting them access to classified information were required to properly store and secure classified information, by Title 18, United States Code, Sections 793 and 1924, and applicable rules, regulations, and orders.

3. Classified information was defined by Executive Order 13526 ("E.O. 13526") and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in E.O. 13526; and (3) is classified by an original classification authority

who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

4. E.O. 13526 also provides that certain senior U.S. officials are authorized to establish "special access programs" upon a finding that "the vulnerability of, or threat to, specific information is exceptional" and "the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure." Within the U.S. Intelligence Community, the Director of National Intelligence is authorized to establish special access programs for intelligence sources, methods, and activities. Such intelligence programs are called "Sensitive Compartmented Information Programs" or SCI Programs. A term commonly used to describe certain materials in such programs is "code word."

5. Pursuant to E.O. 13526, a person may gain access to classified information only if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a "need-to-know" the information.

6. “Need-to-know” means a determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized government function.

7. The classified information being accessed may not be removed from the controlling agency’s premises without permission. Moreover, even when SCI is maintained on the controlling agency’s premises, it must be stored in a Sensitive Compartmented Information Facility (“SCIF”), which is an accredited area, room, group of rooms, building, or installation designed to prevent as well as detect visual, acoustical, technical, and physical access by unauthorized persons.

#### **The Department of Defense**

8. The Department of Defense (“DOD”) was a United States government military agency. The DOD’s headquarters were at Arlington, Virginia. The DOD was responsible for providing the military forces needed to deter war and protect the security of the United States. Moreover, through its subordinate national intelligence services, including the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office, the DOD was responsible for, among other things, collecting information that revealed the military plans, intentions, and capabilities of the United States’ adversaries and the bases for their decisions and actions, as well as conducting clandestine actions, at the direction of the President and his authorized designee, designed to preempt threats and achieve the United States’ policy objectives.

9. The responsibilities of certain DOD employees required that their association with the DOD be kept secret; as a result, the fact that these individuals were employed by the DOD

was classified. The responsibilities of other DOD employees required that, while their employment by the DOD was itself not secret, their association with certain DOD programs and their particular activities on behalf of the DOD were kept secret; accordingly, such information was classified. Disclosure of the fact that such individuals were employed by the DOD, associated with certain DOD programs, or engaged in particular activities on behalf of the DOD, had the potential to damage national security in ways that ranged from preventing the future use of individuals in a covert or clandestine capacity, to compromising clandestine actions and intelligence-gathering methods and operations, to endangering the safety of DOD employees and those who interacted with them.

#### **The Central Intelligence Agency**

10. The CIA was a United States government intelligence agency. The CIA's headquarters were at Langley, Virginia. The CIA was responsible for, among other things, collecting information that revealed the plans, intentions, and capabilities of the United States' adversaries and the bases for their decisions and actions, as well as conducting clandestine actions, at the direction of the President and his authorized designees, designed to preempt threats and achieve the United States' policy objectives.

11. The responsibilities of certain CIA employees required that their association with the CIA be kept secret; as a result, the fact that these individuals were employed by the CIA was classified. The responsibilities of other CIA employees required that, while their employment by the CIA was itself not necessarily secret, their association with certain CIA programs and their particular activities on behalf of the CIA be kept secret; accordingly, such information was classified. Disclosure of the fact that such individuals were employed by the CIA, associated

with certain CIA programs, or engaged in particular activities on behalf of the CIA, had the potential to damage national security in ways that ranged from preventing the future use of individuals in a covert or clandestine capacity, to compromising clandestine actions and intelligence-gathering methods and operations, to endangering the safety of CIA employees and those who dealt with them.

### **Criminal Conduct**

12. Throughout his employment by the DOD, defendant DAVID HOWELL PETRAEUS entered into various agreements with the United States regarding the protection and proper handling of classified information. Examples of these agreements include:

a. On March 15, 2006, as a condition of being granted access to certain SCI, DAVID HOWELL PETRAEUS entered into a Non-Disclosure Agreement ("NDA") with the DOD in which he agreed, in pertinent part, as follows:

I have been advised that unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency . . . that last authorized my access to SCI.

I hereby agree to submit for security review by the [agency] that last authorized my access to such information or material, any writing or other preparation in any form . . . that contains or purports to contain any SCI . . . that I contemplate disclosing to any person not authorized to have access to SCI . . .

In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute a violation or violations of United States criminal laws, including the provisions of . . . Section[ ] 793 . . . [of] Title 18, United States Code . . .

I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity

providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code . . .

Defendant DAVID HOWELL PETRAEUS entered into at least 13 additional NDAs in the course of his DOD employment. In each instance, DAVID HOWELL PETRAEUS promised never to disclose SCI to anyone not authorized to receive it without prior written authorization from the United States government, and he acknowledged that unauthorized retention and/or disclosure of classified information could cause irreparable injury to the United States and be used to advantage by a foreign nation. The scope of these NDAs encompassed classified information referenced in this Statement of Facts.

b. As a condition of being granted access to classified information, defendant DAVID HOWELL PETRAEUS entered into a Secrecy Agreement with the DOD, in which he agreed, in pertinent part, as follows:

I accept the responsibilities associated with being granted access to classified national security information. I am aware of my obligation to protect classified national security information through proper safeguarding and limiting access to individuals with the proper security clearance and official need to know. I further understand that, in being granted access to classified information, a special confidence and trust has been placed in me by the United States Government.

Defendant DAVID HOWELL PETRAEUS entered into at least 13 additional Secrecy Agreements in the course of his DOD employment. In each instance, defendant DAVID HOWELL PETRAEUS agreed to protect classified national security information through proper safeguarding and limiting access to individuals with proper security clearance and official need-to-know.

13. On or about August 31, 2011, defendant DAVID HOWELL PETRAEUS retired from the DOD, after which time he retained his continuing lifelong obligation to the United

States to protect the classified information to which he had been granted access while employed by the DOD.

14. As a condition of his employment by the CIA, defendant DAVID HOWELL PETRAEUS entered into various agreements with the United States, including, for example, the following:

a. On June 16, 2011, as a condition of being granted access to certain SCI, defendant DAVID HOWELL PETRAEUS entered into a NDA with the CIA which was materially identical to the March 2006 NDA he signed while employed by the DOD.

b. On November 26, 2012, following his resignation from the CIA, defendant DAVID HOWELL PETRAEUS entered into a Secrecy Agreement with the CIA in which he agreed, in pertinent part, as follows:

I understand that in the course of my employment . . . I may be given access to information or material that is classified or is in the process of a classification determination . . . that, if disclosed in an unauthorized manner would jeopardize intelligence activities of the United States Government. I accept that by being granted access to such information or material I will be placed in a position of special confidence and trust and become obligated to protect the information and/or material from unauthorized disclosure.

As a further condition of the special confidence and trust reposed in me by the Central Intelligence Agency, I hereby agree to submit for review by the Central Intelligence Agency any writing or other preparation in any form . . . which contains any mention of intelligence data or activities, or contains any other information or material that might be based on [classified information] . . .

I understand that . . . the disclosure of information that I agreed herein not to disclose can, in some circumstances, constitute a criminal offense . . .

15. On or about November 9, 2012, defendant DAVID HOWELL PETRAEUS resigned from the CIA, after which time he retained his continuing lifelong obligation to the

United States to protect the classified information to which he had been granted access while employed by the CIA.

16. During his tenure at the DOD and the CIA, defendant DAVID HOWELL PETRAEUS held a United States government security clearance allowing him access to classified United States government information. As a result, defendant DAVID HOWELL PETRAEUS had regular access to classified and national defense information relating to DOD and CIA programs, operations, methods, sources, and personnel.

17. During his tenure as Commander of ISAF in Afghanistan, defendant DAVID HOWELL PETRAEUS maintained bound, five-by-eight-inch notebooks that contained his daily schedule and classified and unclassified notes he took during official meetings, conferences, and briefings. The notebooks had black covers and, for identification purposes, defendant DAVID HOWELL PETRAEUS taped his business card on the front exterior of each notebook. A total of eight such books (hereinafter the "Black Books") encompassed the period of defendant DAVID HOWELL PETRAEUS's ISAF Command and collectively contained classified information regarding the identities of covert officers, war strategy, intelligence capabilities and mechanisms, diplomatic discussions, quotes and deliberative discussions from high-level National Security Council meetings, and defendant DAVID HOWELL PETRAEUS's discussions with the President of the United States of America.

18. The Black Books contained national defense information, including Top Secret//SCI and code word information.

19. The National Defense University ("NDU") was an institution of higher education funded by the DOD, intended to facilitate high-level training and education, as well as the

development of national security strategy. It was located on the grounds of Fort Lesley McNair, in Washington, D.C. NDU was a repository for the DOD's classified collections.

20. From in or about July 2009 to in or about July 2012, defendant DAVID HOWELL PETRAEUS's DOD historian gathered and organized the classified materials that defendant DAVID HOWELL PETRAEUS collected during his DOD tenure. Defendant DAVID HOWELL PETRAEUS never provided the Black Books to his DOD historian. Instead, defendant DAVID HOWELL PETRAEUS personally retained the Black Books.

21. In or about September 2012, defendant DAVID HOWELL PETRAEUS's DOD historian transferred defendant DAVID HOWELL PETRAEUS's classified collection to NDU for storage and archiving. Because defendant DAVID HOWELL PETRAEUS personally retained the Black Books, they were never transferred to NDU.

22. On or about August 4, 2011, after defendant DAVID HOWELL PETRAEUS returned permanently to the United States from Afghanistan, during a conversation, recorded by his biographer, defendant DAVID HOWELL PETRAEUS stated that the Black Books were "highly classified" and contained "code word" information:

Biographer:	By the way, where are your black books? We never went through. . .
PETRAEUS:	They're in a rucksack up there somewhere.
Biographer:	Okay . . . You avoiding that? You gonna look through 'em first?
PETRAEUS:	Umm, well, they're really -- I mean they are highly classified, some of them. They don't have it on it, but I mean there's code word stuff in there.

23. On or about August 27, 2011, defendant DAVID HOWELL PETRAEUS sent an e-mail to his biographer in which he agreed to provide the Black Books to his biographer.

24. On or about August 28, 2011, defendant DAVID HOWELL PETRAEUS delivered the Black Books to a private residence in Washington, D.C. (the "DC Private Residence"), where his biographer was staying during a week-long trip to Washington, D.C. The DC Private Residence was not approved for the storage of classified information.

25. Thereafter, from on or about August 28, 2011, to on or about September 1, 2011, defendant DAVID HOWELL PETRAEUS left the Black Books at the DC Private Residence in order to facilitate his biographer's access to the Black Books and the information contained therein to be used as source material for his biography, titled *All In: The Education of General David Petraeus*, released by Penguin Press in 2012. No classified information from the Black Books appeared in the aforementioned biography.

26. On or about September 1, 2011, defendant DAVID HOWELL PETRAEUS retrieved the Black Books from the DC Private Residence and returned them to his own Arlington, Virginia home (the "PETRAEUS Residence").

27. On or about November 9, 2012, defendant DAVID HOWELL PETRAEUS resigned from the CIA. Approximately two weeks after his November 9, 2012 resignation, defendant DAVID HOWELL PETRAEUS was debriefed and read-out of the SCI compartments and Special Access Programs to which he previously had been granted access. Specifically, on or about November 26, 2012, defendant DAVID HOWELL PETRAEUS executed two SCI NDAs which contained debriefing acknowledgments, a Secrecy Agreement, and a Security Exit Form. The Security Exit Form included seven provisions regarding his continuing duty to

protect classified information from disclosure. Among other things, by signing the Security Exit Form, defendant DAVID HOWELL PETRAEUS adopted the following provision: "I give my assurance that there is no classified material in my possession, custody, or control at this time." At the time he provided this assurance, the Black Books were still in the PETRAEUS Residence.

28. On or about January 3, 2013, a SCIF, which had been installed at the PETRAEUS Residence by the CIA during defendant DAVID HOWELL PETRAEUS's tenure as CIA Director, was closed and de-accredited. The SCIF was subsequently removed on or about February 13, 2013.

29. On or about April 5, 2013, the FBI executed a court-authorized search warrant at the PETRAEUS Residence and seized the Black Books from an unlocked desk drawer in the first-floor study of the PETRAEUS Residence.

30. Between in or about August 2011, and on or about April 5, 2013, defendant DAVID HOWELL PETRAEUS, being an employee of the United States, and by virtue of his employment, became possessed of documents and materials containing classified information of the United States, and did unlawfully and knowingly remove such documents and materials without authority and thereafter intentionally retained such documents and materials at the DC Private Residence and the PETRAEUS Residence, aware that these locations were unauthorized for the storage and retention of such classified documents and materials.

31. On or about June 12, 2012, in two separate interviews conducted by special agents of the Federal Bureau of Investigation ("FBI") regarding investigations unrelated to the instant offense, defendant DAVID HOWELL PETRAEUS acknowledged that he understood that making false statements to the FBI in the course of a criminal investigation was a crime.

Specifically, on June 12, 2012, defendant DAVID HOWELL PETRAEUS was interviewed in his office at CIA Headquarters in Langley, Virginia, in connection with two media leak investigations. During both interviews, defendant DAVID HOWELL PETRAEUS affirmed in writing, "I understand that providing false statements to the Federal Bureau of Investigation is a violation of law."

32. On or about October 26, 2012, defendant DAVID HOWELL PETRAEUS was interviewed by two FBI special agents in his office at CIA Headquarters in Langley, Virginia. Defendant DAVID HOWELL PETRAEUS was advised that the special agents were conducting a criminal investigation. During that interview, the special agents questioned DAVID HOWELL PETRAEUS about the mishandling of classified information. In response to those questions, defendant DAVID HOWELL PETRAEUS stated that (a) he had never provided any classified information to his biographer, and (b) he had never facilitated the provision of classified information to his biographer. These statements were false. Defendant DAVID HOWELL PETRAEUS then and there knew that he previously shared the Black Books with his biographer.

33. The acts taken by defendant DAVID HOWELL PETRAEUS were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

34. This Statement of Facts includes those facts necessary to support the Plea Agreement between the defendant and the government. It does not include each and every fact known to the defendant or to the government, and it is not intended to be a full enumeration of all the facts surrounding defendant DAVID HOWELL PETRAEUS's case.

//

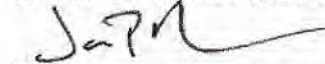
//

**United States Sentencing Guidelines**

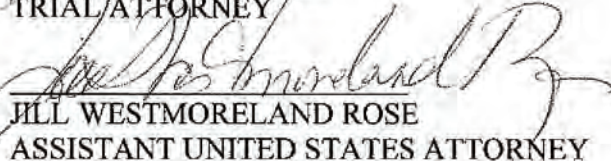
35. Further, in accordance with Fed. R. Crim. P. 11(c)(1)(B) of the Federal Rules of Criminal Procedure, the United States and the defendant will recommend to the Court that the following provisions of the United States Sentencing Guidelines apply:

Base Offense Level:	6	[U.S.S.G. § 2X5.2]
Abuse of Position of Trust:	+2	[U.S.S.G. § 3B1.3]
Obstruction of Justice	+2	[U.S.S.G. § 3C1.1]
Acceptance of Responsibility	-2	[U.S.S.G. § 3E1.1(a)]
<b>Total Adjusted Offense Level</b>	<b>8</b>	

ANNE M. TOMPKINS  
UNITED STATES ATTORNEY



JAMES P. MELENDRES  
TRIAL ATTORNEY



JILL WESTMORELAND ROSE  
ASSISTANT UNITED STATES ATTORNEY

  
RICHARD S. SCOTT  
TRIAL ATTORNEY

2/23/2015

Feb. 23, 2015

2/23/2015

//

//

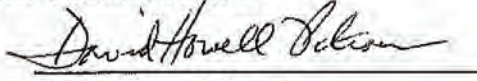
//

//

//

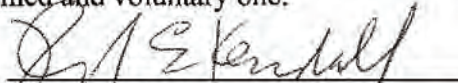
Defendant's Signature: After consulting with my attorney, and pursuant to the Plea Agreement entered into this day between myself and the United States, I hereby stipulate that the above Factual Basis is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 22 February 2015

  
David Howell Petraeus  
Defendant

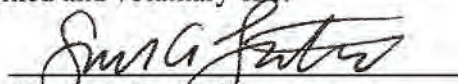
Defense Counsel Signature: I am counsel for the defendant in this case. I carefully reviewed the above Factual Basis with the defendant. To my knowledge, the defendant's decision to stipulate to these facts is an informed and voluntary one.

Date: Feb 23, 2015

  
David E. Kendall  
Williams & Connolly LLP  
Counsel for the Defendant

Defense Counsel Signature: I am counsel for the defendant in this case. I carefully reviewed the above Factual Basis with the defendant. To my knowledge, the defendant's decision to stipulate to these facts is an informed and voluntary one.

Date: Feb. 23, 2015

  
Simon A. Latcoyich  
Williams & Connolly LLP  
Counsel for the Defendant

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF NORTH CAROLINA  
CHARLOTTE DIVISION

FILED  
CHARLOTTE, NC  
MAR 3 2015

U.S. DISTRICT COURT  
WESTERN DISTRICT OF NC

UNITED STATES OF AMERICA

v.

DAVID HOWELL PETRAEUS

) DOCKET NO.: 3:15 CR 47

) PLEA AGREEMENT

NOW COMES the United States of America, by and through Anne M. Tompkins, United States Attorney for the Western District of North Carolina, James P. Melendres, Trial Attorney, Jill Westmoreland Rose, Assistant United States Attorney, and Richard S. Scott, Trial Attorney, the defendant, David Howell Petraeus, and the defendant's counsel, David E. Kendall and Simon A Latcovich, and respectfully inform the Court that they have reached an agreement pursuant to Federal Rule of Criminal Procedure 11. References to the United States herein shall mean the United States Attorney for the Western District of North Carolina.

**I. Plea**

1. The defendant agrees to enter a voluntary plea of guilty to Count ONE as set forth in the Bill of Information, and admits to being in fact guilty as charged in Count ONE.

2. The defendant understands that each and every provision set forth below is a material term of the Plea Agreement. The defendant's failure to fully comply with any provision of the Plea Agreement, attempt to withdraw the guilty plea or violation of any federal, state, or local law, or any order of any court, including any condition of pre-trial or pre-sentence, or post-sentence release is a breach of the Plea Agreement. In addition to any other remedy available in law, the defendant's breach (i) will relieve the United States of its obligations under the Plea Agreement, but the defendant will not be relieved of the defendant's obligations or allowed to withdraw the guilty plea; (ii) may constitute the defendant's failure to accept responsibility under United States Sentencing Guideline ("U.S.S.G.") § 3E1.1; and (iii) will permit the United States to proceed on any dismissed, pending, superseding, or additional charges.

**II. Venue Waiver**

3. The United States and the defendant agree and stipulate that this District is an appropriate venue for entry of a plea by the defendant to a Bill of Information charging a violation of 18 U.S.C. § 1924.

**III. Sentence**

4. The defendant is aware that the statutory maximum sentence for Count ONE is as follows:

Count ONE: a violation of 18 U.S.C. § 1924; a maximum term of one year imprisonment, a \$100,000 fine, or both, a special assessment of \$25, and no more than 5 years of probation.

5. The defendant understands that a violation of any terms or conditions of supervised release, should it be imposed, may subject the defendant to an additional period of incarceration.

6. The defendant is aware that the Court: (a) will consider the advisory U.S.S.G. in determining the sentence; (b) has not yet determined the sentence and any estimate of the likely sentence is a prediction rather than a promise; (c) has the final discretion to impose any sentence up to the statutory maximum; and (d) is not bound by recommendations or agreements by the United States. Knowing this, the defendant understands that the defendant may not withdraw the plea as a result of the sentence imposed.

7. Pursuant to Fed. R. Crim. P. 11(c)(1)(B), the parties agree that they will jointly recommend that the Court make the following findings and conclusions as to the U.S.S.G:

a. The offense level for the subject offense is as follows:

Base Offense Level:	6	[U.S.S.G. § 2X5.2]
Abuse of Position of Trust:	+2	[U.S.S.G. § 3B1.3]
Obstruction of Justice	+2	[U.S.S.G. § 3C1.1]
Acceptance of Responsibility	-2	[U.S.S.G. § 3E1.1]
<b>Total Adjusted Offense Level</b>	<b>8</b>	

b. Unless otherwise set forth herein, the parties agree that they will make the above recommendations as to the adjusted offense level, and will recommend no other enhancements or reductions to the Court.

8. The United States agrees not to oppose the defendant's request that the defendant receive a non-custodial sentence.

9. The parties jointly recommend the imposition of a two-year term of probation.

10. The parties jointly recommend the imposition of a \$40,000 fine.

11. The parties jointly waive the preparation of a Pre-Sentence Report. However, the defendant expressly acknowledges that the Court is not bound by this waiver and recommendation. The parties will inform the Court and the United States Probation Office of all facts pertinent to the sentencing process and will present any evidence requested by the Court.

12. The defendant agrees to the following with respect to financial disclosures, monetary penalties, forfeiture, and restitution:

a. To make full payment of such fine as the Court may impose, within one week of the sentencing hearing. If such full payment is not made within one week of sentencing hearing, to make full disclosure of all current and projected assets to the U.S. Probation Office immediately and prior to the termination of the defendant's supervised release or probation, such disclosures to be shared with the U.S. Attorney's Office, including the Financial Litigation Unit, for any purpose.

b. That monetary penalties imposed by the Court will be (i) subject to immediate enforcement as provided for in 18 U.S.C. § 3613, and (ii) submitted to the Treasury Offset Program so that any federal payment or transfer of returned property the defendant receives may be offset and applied to federal debts but will not affect the periodic payment schedule.

#### **IV. Immunity from Further Prosecution in This District and Others**

13. The United States will not bring any additional criminal charges against the defendant for the conduct outlined in the Factual Basis or for any other criminal offenses committed by the defendant which are known to the United States at the time of disposition.

#### **V. Procedure**

14. The defendant will plead guilty because the defendant is in fact guilty of the charged offense. The defendant admits the facts set forth in the Factual Basis filed with this Plea Agreement and agrees that those facts establish guilt of the offense charged beyond a reasonable doubt. The Factual Basis, which is hereby incorporated into this Plea Agreement, constitutes a stipulation of facts for purposes of § 1B1.2(a) of the U.S.S.G. and Fed. R. Crim. P. 11(b)(3).

15. The defendant further stipulates that the Factual Basis may be used by the Court and the United States Probation Office without objection by the defendant to determine the applicable advisory guideline range or the appropriate sentence under 18 U.S.C. § 3553(a).

#### **VI. Waivers**

16. The defendant is aware that the law provides certain limited rights to withdraw a plea of guilty, has discussed these rights with defense counsel and knowingly and expressly waives any right to withdraw the plea once the Court has accepted it.

17. The defendant acknowledges that Fed. R. Crim. P. 11(f) and Fed. R. of Evid. 408 and 410 are rules which ordinarily limit the admissibility of statements made by a defendant in the course of plea discussions. The defendant knowingly and voluntarily waives these rights and

agrees that any statements made in the course of the defendant's guilty plea or this Plea Agreement (in part or in its entirety, at the sole discretion of the United States) will be admissible against the defendant for any purpose in any criminal or civil proceeding if the defendant fails to enter or attempts to withdraw the defendant's guilty plea, or in any post-conviction proceeding challenges the voluntary nature of the guilty plea.

18. The defendant agrees that by pleading guilty, the defendant is expressly waiving the right: (a) to be tried by a jury; (b) to be assisted by an attorney at trial; (c) to confront and cross-examine witnesses; and (d) not to be compelled to incriminate himself.

19. The defendant has discussed with his attorney: (1) defendant's rights pursuant to 18 U.S.C. § 3742, 28 U.S.C. § 2255, and similar authorities to contest a conviction and/or sentence through an appeal or post-conviction after entering into a Plea Agreement; (2) whether there are potential issues relevant to an appeal or post-conviction action; and (3) the possible impact of any such issue on the desirability of entering into this Plea Agreement.

20. The defendant, in exchange for the concessions made by the United States in this Plea Agreement, waives all such rights to contest the conviction except for: (1) claims of ineffective assistance of counsel or (2) prosecutorial misconduct. The defendant also knowingly and expressly waives all rights conferred by 18 U.S.C. § 3742 or otherwise to appeal whatever sentence is imposed with the two exceptions set forth above. The defendant agrees that the United States preserves all its rights and duties as set forth in 18 U.S.C. § 3742(b).

21. The defendant waives all rights, whether asserted directly or by a representative, to request or to receive from any department or agency any records pertaining to the investigation or prosecution of this case, including without limitation any records that may be sought under the Freedom of Information Act, 5 U.S.C. § 552, or the Privacy Act, 5 U.S.C. § 552a.

## VII. Conclusion

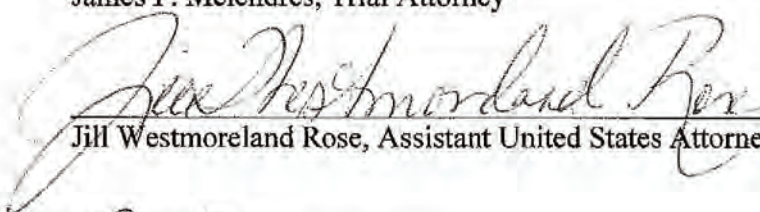
22. This agreement is effective and binding once signed by the defendant, the defendant's attorney, and an attorney for the United States. The defendant agrees to entry of this Plea Agreement at the date and time scheduled by the Court.

23. There are no agreements, representations, or understandings between the parties in this case, other than those explicitly set forth in this Plea Agreement, or as noticed to the Court during the plea colloquy and contained in writing in a separate document signed by all parties.

SO AGREED:

  
James P. Melendres, Trial Attorney


DATED: 2/23/2015

  
Jill Westmoreland Rose, Assistant United States Attorney

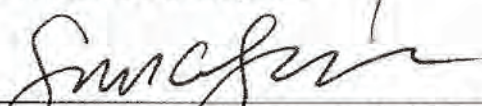
DATED: Feb. 23, 2015

  
Richard S. Scott, Trial Attorney

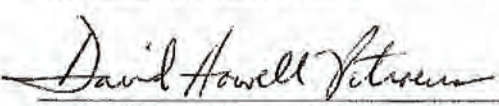
DATED: 2/23/2015

  
David E. Kendall, Attorney for Defendant  
Williams & Connolly LLP

DATED: Feb 23, 2015

  
Simon A. Latcovich, Attorney for Defendant  
Williams & Connolly LLP

DATED: Feb. 23, 2015

  
David Howell Petraeus, Defendant

DATED: 22 February 2015

Revised January 2015